**Test\_2015-01-15-1052**

**[project ID not provided]**

**Security Assessment Report**

**(SAR)**

Prepared for

**Department of Homeland Security Headquarters (DHS HQ)**

**[Component address not provided]**

**[project version not provided]**

**16 January 2015**

EXECUTIVE SUMMARY

This security assessment performed on the Test\_2015-01-15-1052 follows guidance from the National Institute of Standards and Technology (NIST) Special Publication 800-30, *Guide for Conducting Risk Assessments*, and incorporates policy from the Department of Homeland Security (DHS)Sensitive Systems Policy Directive 4300A and the DHS 4300A Sensitive Systems Handbook (4300A SSH).

The security assessment was performed by Department of Homeland Security Headquarters (DHS HQ).

Table of Contents

[1.0 Introduction 1](#_Toc256000000)

[1.1 Purpose 1](#_Toc256000001)

[1.2 Scope 1](#_Toc256000002)

[1.3 System Data 1](#_Toc256000003)

[1.4 Team Composition 1](#_Toc256000004)

[1.5 Assumptions and Constraints 1](#_Toc256000005)

[1.6 Risk Rating Scale 1](#_Toc256000006)

[2.0 Security Assessment Results 2](#_Toc256000007)

[3.0 Conclusion 3](#_Toc256000009)

[3.1 Statement of Residual Risk 331](#_Toc256000010)

[3.2 Level of Acceptable Risk 331](#_Toc256000011)

[3.3 Security Control Assessor Recommendation to AO 331](#_Toc256000012)

# 1.0 Introduction

This Security Assessment Report was developed from the Test\_2015-01-15-1052 activities associated with the security authorization process using guidance contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 1, *Guidelines for Applying the Risk Management Framework to Federal Information Systems.*

## 1.1 Purpose

The purpose of this report is to identify to the Authorizing Official (AO) and the System Owner (SO) the results of a Security Assessment performed on the system. The Security Assessment consists of the system Risk Assessment, Security Assessment Plan, and Contingency Plan Test.

## 1.2 Scope

Test\_2015-01-15-1052 is hosted:

**Table 1-1: System Resident Information**

|  |  |
| --- | --- |
| **System Site** | **Facility Location** |
| Main Location | City Not Provided , State Not Provided |

## 1.3 System Data

Table 1-2: FIPS 199 Categorization Summary

|  |  |
| --- | --- |
| **Security Objective** | **Security Impact Level** |
| Confidentiality | High |
| Integrity | High |
| Availability | High |

## 1.4 Team Composition

NO Assessment personnels defined in the Project Personnel page.

## 1.5 Assumptions and Constraints

The following assumptions and constraints apply to this document:

## 1.6 Risk Rating Scale

Table 1-4: Risk Rating Scale

|  |  |
| --- | --- |
| Rating | Description |
| LOW | The system’s AO must determine whether corrective actions are still required or decide to accept the risk.  Risk may be acceptable according to the system sensitivity and criticality.  Risk is probably acceptable for short term until cost effective safeguards can be implemented. |
| MODERATE | Probability of incident is elevated, with increased probability of unauthorized disclosure or Denial Of Service (DoS) of critical systems.  Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.  Risks are probably not acceptable according to the system sensitivity and criticality. |
| HIGH | There is a strong need for corrective measures.  An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.  Probability of serious incident is likely. Risks not normally acceptable, according to the system sensitivity and criticality.  Authorization status may be rescinded or not granted. |

# 2.0 Security Assessment Results

494 controls have been identified as being applicable to this system and 522 Tests were evaluated:

* 0 tests were implemented correctly, operating as intended, and producing the desired outcome, meeting the security requirements for the system.
* 522 Tests were failed, producing a total of 494 risks.
  + 494 test result(s) present a High risk to system operation.
  + 0 test result(s) present a Moderate risk to system operation.
  + 0 test result(s) present a Low risk to system operation.
* 0 tests were found to be Not Applicable

The total risk level is High.

# 

# 3.0 Conclusion

**Table 3-1: Risks that must be Remediated within 30 days of ATO or Receive an Exception/Waiver Prior to ATO**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Exception / Waiver | Traceability | Risks | Affected Elements | Risk Level | Recommended Remediation | Compensating Measure |
| [E-# OR W-#] | Water Damage Protection [NIST 800-53 w/ DHS 4300A PE-15] | [Test: PE-15.1 - Water Damage Protection]  Not Entered | Failure to ensure that the organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel could lead to the compromise of the system or of the data in the system. | High | [Test: PE-15.1 - Water Damage Protection]  Not Entered |  |
| [E-# OR W-#] | Security Assessment and Authorization Policies and Procedures [NIST 800-53 w/ DHS 4300A CA-1] | [Test: CA-1.1 - Security Assessment and Authorization Policies and Procedures]  Not Entered  [Test: CA-1.2 - Security Assessment and Authorization Policies and Procedures]  Not Entered | Failure to meet the certification, accreditation, and security assessment policies and procedures requirements listed below could result in a weak security stance of the organization due to security threats that may not have been addressed accordingly or completely by organizational personnel with certification, accreditation and assessment roles and responsibilities:  (i) the organization defines the frequency of security assessment and authorization policy reviews/updates; (ii) the organization reviews/updates security assessment and authorization policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of security assessment and authorization procedure reviews/updates; and (iv) the organization reviews/updates security assessment and authorization procedures in accordance with organization-defined frequency.  Failure to meet the certification, accreditation, and security assessment policies and procedures requirements listed below could result in a weak security stance of the organization due to the lack of current or improved certification and assessment information:  (i) the organization develops and formally documents security assessment and authorization policy; (ii) the organization security assessment and authorization policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented security assessment and authorization policy to elements within the organization having associated security assessment and authorization roles and responsibilities; (iv) the organization develops and formally documents security assessment and authorization procedures; (v) the organization security assessment and authorization procedures facilitate implementation of the security assessment and authorization policy and associated security assessment and authorization controls; and (vi) the organization disseminates formal documented security assessment and authorization procedures to elements within the organization having associated security assessment and authorization roles and responsibilities. | High | [Test: CA-1.1 - Security Assessment and Authorization Policies and Procedures]  Not Entered  [Test: CA-1.2 - Security Assessment and Authorization Policies and Procedures]  Not Entered |  |
| [E-# OR W-#] | Senior Information Security Officer [NIST 800-53 w/ DHS 4300A PM-2] | [Test: PM-2.1 - Senior Information Security Officer]  Not Entered | Failure to to ensure that the organization appoints a senior information security officer with the mission and resources to coordinate, develop, implement, and maintain an organization-wide information security program could lead to the organization's mismanagement of the information security program. | High | [Test: PM-2.1 - Senior Information Security Officer]  Not Entered |  |
| [E-# OR W-#] | Information Security Program Plan [NIST 800-53 w/ DHS 4300A PM-1] | [Test: PM-1.1 - Information Security Program Plan]  Not Entered | Failure to meet the information security program plan requirements indicated below could lead to the exposure of the confidentiality, integrity and availability of data information and system:  (i) the organization develops and disseminates an organization-wide information security program plan that:   * provides an overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements; * includes the identification and assignment of roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and * is approved by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation;   (ii) the organization defines the frequency of the organization-wide information security program plan reviews;   (iii) the organization updates the plan to address organizational changes and problems identified during plan implementation or security control assessments; and  (iv) the organization protects the information security program plan from unauthorized disclosure and modification. | High | [Test: PM-1.1 - Information Security Program Plan]  Not Entered |  |
| [E-# OR W-#] | Identifier Management [NIST 800-53 w/ DHS 4300A IA-4] | [Test: IA-4.1 - Identifier Management]  Not Entered | Failure to meet the identifier management requirements listed below could expose information system to unauthorized access and lead to compromise of information system integrity and confidentiality:  (i) the organization defines the time period for preventing reuse of user or device identifiers; (ii) the organization defines the time period of inactivity after which a user identifier is to be disabled; and (iii) the organization manages information system identifiers for users and devices by:   * receiving authorization from a designated organizational official to assign a user or device identifier; * selecting an identifier that uniquely identifies an individual or device; * assigning the user identifier to the intended party or the device identifier to the intended device; * preventing reuse of user or device identifiers for the organization-defined time period; and * disabling the user identifier after the organization-defined time period of inactivity. | High | [Test: IA-4.1 - Identifier Management]  Not Entered |  |
| [E-# OR W-#] | Personnel Security Policy and Procedures [NIST 800-53 w/ DHS 4300A PS-1] | [Test: PS-1.1 - Personnel Security Policy and Procedures]  Not Entered  [Test: PS-1.2 - Personnel Security Policy and Procedures]  Not Entered | Failure to meet the personnel security policy and procedures requirements listed below could result in the incomplete and ineffective personnel security policy and procedures leaving the personnel/employee with a different interpretation of the policy, which could lead to the abuse of information system resources and possibly to the compromise of the system or data:  (i) the organization defines the frequency of personnel security policy reviews/updates; (ii) the organization reviews/updates personnel security policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of personnel security procedure reviews/updates; (iv) the organization reviews/updates personnel security procedures in accordance with organization-defined frequency.  Failure to meet the personnel security policy and procedures requirements listed below could result in the personnel/employee being unaware of the existing personnel security policy and procedures, which could lead to the abuse of information system resources and possibly to the compromise of the system or data:  (i) the organization develops and formally documents personnel security policy; (ii) the organization personnel security policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented personnel security policy to elements within the organization having associated personnel security roles and responsibilities; (iv) the organization develops and formally documents personnel security procedures; (v) the organization personnel security procedures facilitate implementation of the personnel security policy and associated personnel security controls; and (vi) the organization disseminates formal documented personnel security procedures to elements within the organization having associated personnel security roles and responsibilities. | High | [Test: PS-1.1 - Personnel Security Policy and Procedures]  Not Entered  [Test: PS-1.2 - Personnel Security Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Critical Infrastructure Plan [NIST 800-53 w/ DHS 4300A PM-8] | [Test: PM-8.1 - Critical Infrastructure Plan]  Not Entered | Failure to ensure that the organization addresses information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: PM-8.1 - Critical Infrastructure Plan]  Not Entered |  |
| [E-# OR W-#] | DHS owned Removable Media [NIST 800-53 w/ DHS 4300A MP-7 (DHS-4.3.1.e)] | [Test: MP-7(DHS-4.3.1.e) - DHS owned Removable Media]  Not Entered | Failure to ensure that the DHS-owned removable media is not connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM) could result in the disclosure of critical and sensitive mission/business information that may have been contained in the media. | High | [Test: MP-7(DHS-4.3.1.e) - DHS owned Removable Media]  Not Entered |  |
| [E-# OR W-#] | Audit Record Retention [NIST 800-53 w/ DHS 4300A AU-11] | [Test: AU-11.1 - Audit Record Retention]  Not Entered | Failure to meet the audit record retention requirements listed below could result in the loss of the generated audit data, which could render an audit or forensic investigation efforts useless:  (i) the organization defines the retention period for audit records; (ii) the retention period for audit records is consistent with the records retention policy; and, (iii) the organization retains audit records for the organization-defined time period consistent with the records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. | High | [Test: AU-11.1 - Audit Record Retention]  Not Entered |  |
| [E-# OR W-#] | Publicly Accessible Content [NIST 800-53 w/ DHS 4300A AC-22] | [Test: AC-22.1 - Publicly Accessible Content]  Not Entered | Failure to meet the publicly accessible content requirements listed below could leave essential data exposed to unauthorized access and viewing by individuals not connected to the organization:  (i) the organization designates individuals authorized to post information onto an organizational information system that is publicly accessible; (ii) the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; (iii) the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; (iv) the organization defines the frequency of reviews of the content on the publicly accessible organizational information system for nonpublic information; (v) the organization reviews the content on the publicly accessible organizational information system for nonpublic information in accordance with the organization-defined frequency; and (vi) the organization removes nonpublic information from the publicly accessible organizational information system, if discovered. | High | [Test: AC-22.1 - Publicly Accessible Content]  Not Entered |  |
| [E-# OR W-#] | Privacy Incident Response [NIST 800-53 w/ DHS 4300A PRIV-SE-2] | [Test: SE-2.1 - Privacy Incident Response]  Not Entered | Failure to meet the privacy incident response requirements listed below could lead PII issues and concerns left unattended and may cause disruption of critical mission/business functions, operations, and processes due to the ineffective contingency plans:  (i) the organization develops and implements a Privacy Incident Response Plan; and (ii) the organization provides an organized and effective response to privacy incidents in accordance with the organizational Privacy Incident Response Plan. | High | [Test: SE-2.1 - Privacy Incident Response]  Not Entered |  |
| [E-# OR W-#] | Incident Reporting [NIST 800-53 w/ DHS 4300A IR-6] | [Test: IR-6.1 - Incident Reporting]  Not Entered | Failure to meet the requirements for incident reporting listed below could lead to the compromise the system or the misuse of data being processed, transported, or stored inside the system:  (i) the organization defines in the time period required to report suspected security incidents to the organizational incident response capability; (ii) the organization requires personnel to report suspected security incidents to the organizational incident response capability within the organization-defined time period; and (iii) the organization reports security incident information to designated authorities. | High | [Test: IR-6.1 - Incident Reporting]  Not Entered |  |
| [E-# OR W-#] | Minimization of Personally Identifiable Information [NIST 800-53 w/ DHS 4300A PRIV-DM-1] | [Test: DM-1.1 - Minimization of Personally Identifiable Information]  Not Entered | Failure to meet the data minimization and retention requirements listed below could lead to the compromise or unauthorized disclosure of personally identifiable information:  (i) the organization identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; (ii) the organization limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and, (iii) the organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings , at least annually, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. | High | [Test: DM-1.1 - Minimization of Personally Identifiable Information]  Not Entered |  |
| [E-# OR W-#] | Personnel Sanctions [NIST 800-53 w/ DHS 4300A PS-8] | [Test: PS-8.1 - Personnel Sanctions]  Not Entered | Failure to meet the personnel sanctions requirements indicated below could put the organization at greater security risk:  (i) the organization employs a formal sanctions process for individuals failing to comply with established information security policies and procedures; and  (ii) the organization notifies organization-defined personnel or roles within organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. | High | [Test: PS-8.1 - Personnel Sanctions]  Not Entered |  |
| [E-# OR W-#] | Contacts with Security Groups and Associations [NIST 800-53 w/ DHS 4300A PM-15] | [Test: PM-15.1 - Contacts with Security Groups and Associations]  Not Entered | Failure to ensure that the organization establishes and institutionalizes contact with selected groups and associations within the security community that are indicated below could result in the ignorance of basic security practices, which could be taken advantage of by would-be attackers seeking to break into the information system of the organization through several foot-printing methods including, but not limited to, phishing and social engineering:  (i) To facilitate ongoing security education and training for organizational personnel;  (ii) To maintain currency with recommended security practices, techniques, and technologies; and  (iii) To share current security-related information including threats, vulnerabilities, and incidents. | High | [Test: PM-15.1 - Contacts with Security Groups and Associations]  Not Entered |  |
| [E-# OR W-#] | Unsuccessful Logon Attempts [NIST 800-53 w/ DHS 4300A AC-7] | [Test: AC-7.1 - Unsuccessful Logon Attempts]  Not Entered | Failure to meet the unsuccessful login attempts requirements indicated below could enable would-be attackers to launch dictionary-based attacks or "brute force" attacks against the system to try and get access to system resources and cause damage to the information system:  (i) the organization defines the maximum number of consecutive invalid login attempts to the information system by a user and the time period in which the consecutive invalid attempts occur; (ii) the information system enforces the organization-defined limit of consecutive invalid login attempts by a user during the organization-defined time period; (iii) the organization defines action to be taken by the system when the maximum number of unsuccessful login attempts is exceeded as:   * lock out the account/node for a specified time period; * lock out the account/note until released by an administrator; or * delay the next login prompt according to organization-defined delay algorithm;   (iv) the information system either automatically locks the account/node for the organization-defined time period, locks the account/node until released by an administrator, or delays next login prompt for the organization-defined delay period when the maximum number of unsuccessful login attempts is exceeded; and (v) the information system performs the organization-defined actions when the maximum number of unsuccessful login attempts is exceeded regardless of whether the login occurs via a local or network connection. | High | [Test: AC-7.1 - Unsuccessful Logon Attempts]  Not Entered |  |
| [E-# OR W-#] | Controlled Maintenance [NIST 800-53 w/ DHS 4300A MA-2] | [Test: MA-2.1 - Controlled Maintenance]  Not Entered | Failure of the organization to schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements could lead eventually to the system losing its stability or its integrity:  (i) the organization schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; (ii) the organization controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location; (iii) the organization requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs; (iv) the organization sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and (v) the organization checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions. | High | [Test: MA-2.1 - Controlled Maintenance]  Not Entered |  |
| [E-# OR W-#] | Access Enforcement [NIST 800-53 w/ DHS 4300A AC-3] | [Test: AC-3.1 - Access Enforcement]  Not Entered | Failure to ensure that the information system enforces approved authorizations for logical access to the system in accordance with applicable policy could allow the system to become vulnerable to unauthorized access via improper account use. | High | [Test: AC-3.1 - Access Enforcement]  Not Entered |  |
| [E-# OR W-#] | System of Records Notices and Privacy Act Statements [NIST 800-53 w/ DHS 4300A PRIV-TR-2] | [Test: TR-2.1 - System of Records Notices and Privacy Act Statements]  Not Entered | Failure to meet the transparency requirements listed below increases the risk to unauthorized disclosure of personally identifiable information:  (i) the organization publishes System of Records Notices (SORNs) in the Federal Register, subject to required oversight processes, for systems containing personally identifiable information (PII); (ii) the organization keeps SORNs current; and (iii) the organization includes Privacy Act Statements on its forms that collect PII, or on separate forms that can be retained by individuals, to provide additional formal notice to individuals from whom the information is being collected. | High | [Test: TR-2.1 - System of Records Notices and Privacy Act Statements]  Not Entered |  |
| [E-# OR W-#] | Fire Protection [NIST 800-53 w/ DHS 4300A PE-13] | [Test: PE-13.1 - Fire Protection]  Not Entered | Failure to ensure that the organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source could lead to the disruption of critical mission/business operations. | High | [Test: PE-13.1 - Fire Protection]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2] | [Test: CP-2.1 - Contingency Plan]  Not Entered  [Test: CP-2.2 - Contingency Plan]  Not Entered | Failure to meet the contingency plan requirements listed below could leave the organization unprepared for any incident when it occurs due to incomplete or inaccurate plan and procedures, which could lead to the compromise of the system or of the data in the system:  (i) the organization coordinates contingency planning activities with incident handling activities: (ii) the organization defines the frequency of contingency plan reviews; (iii) the organization reviews the contingency plan for the information system in accordance with the organization-defined frequency; (iv) the organization revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution or testing; and (v) the organization communicates contingency plan changes to the key contingency personnel and organizational elements as identified in CP-2.1 (ii).  Failure to meet the requirements for contingency planning listed below could lead to the compromise of the system or of the data in the system:  (i) the organization develops a contingency plan for the information system that:   * identifies essential missions and business functions and associated contingency requirements; * provides recovery objectives, restoration priorities, and metrics; * addresses contingency roles, responsibilities, assigned individuals with contact information; * addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; and * addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and * is reviewed and approved by designated officials within the organization;   (ii) the organization defines key contingency personnel (identified by name and/or by role) and organizational elements designated to receive copies of the contingency plan; and (iii) the organization distributes copies of the contingency plan to organization-defined key contingency personnel and organizational elements. | High | [Test: CP-2.1 - Contingency Plan]  Not Entered  [Test: CP-2.2 - Contingency Plan]  Not Entered |  |
| [E-# OR W-#] | Governance and Privacy Program [NIST 800-53 w/ DHS 4300A PRIV-AR-1] | [Test: AR-1.1 - Governance and Privacy Program]  Not Entered | Failure to meet the governance and privacy program requirements listed below could leave the organization unprepared for any incident when it occurs, which could lead to the compromise or unauthorized disclosure of personally identifiable information:  (i) the organization appoints a Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) accountable for developing, implementing, and maintaining an organization-wide governance and privacy program to ensure compliance with all applicable laws and regulations regarding the collection, use, maintenance, sharing, and disposal of personally identifiable information (PII) by programs and information systems; (ii) the organization monitors federal privacy laws and policy for changes that affect the privacy program; (iii) the organization allocates sufficient budget and staffing resources to implement and operate the organization-wide privacy program; (iv) the organization develops a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures; (v) the organization develops, disseminates, and implements operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII; and, (vi) the organization updates privacy plan, policies, and procedures at least biennially. | High | [Test: AR-1.1 - Governance and Privacy Program]  Not Entered |  |
| [E-# OR W-#] | Collaborative Computing Devices [NIST 800-53 w/ DHS 4300A SC-15] | [Test: SC-15.1 - Collaborative Computing Devices]  Not Entered | Failure to meet the collaborative computing devices indicated below could lead to disclosure of information that could be used by an attacker for further attacks:  (i) the information system prohibits remote activation of collaborative computing devices with the organization-defined exceptions where remote activation is to be allowed; and  (ii) the information system provides an explicit indication of use to users physically present at the devices. | High | [Test: SC-15.1 - Collaborative Computing Devices]  Not Entered |  |
| [E-# OR W-#] | Contingency Training [NIST 800-53 w/ DHS 4300A CP-3] | [Test: CP-3.1 - Contingency Training]  Not Entered | Failure to meet the contingency training requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization provides initial contingency training to personnel with contingency roles and responsibilities with respect to the information system; (ii) the organization defines the frequency of refresher contingency training; and (iii) the organization provides refresher training in accordance with organization-defined frequency. | High | [Test: CP-3.1 - Contingency Training]  Not Entered |  |
| [E-# OR W-#] | Monitoring Physical Access [NIST 800-53 w/ DHS 4300A PE-6] | [Test: PE-6.1 - Monitoring Physical Access]  Not Entered | Failure to meet the requirements for monitoring physical access listed below could lead to the compromise of the system or of the data in the system:  (i) the organization monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; (ii) the organization reviews physical access logs organization-defined frequency and upon occurrence of organization-defined events or potential indications of events; and (iii) the organization coordinates results of reviews and investigations with the organizational incident response capability. | High | [Test: PE-6.1 - Monitoring Physical Access]  Not Entered |  |
| [E-# OR W-#] | Information Sharing with Third Parties [NIST 800-53 w/ DHS 4300A PRIV-UL-2] | [Test: UL-2.1 - Information Sharing with Third Parties]  Not Entered | Failure to meet the use limitation requirements listed below increases the risk to loss, unauthorized access, or disclosure of privacy information:  (i) the organization shares personally identifiable information (PII) externally, only for the authorized purposes identified in the Privacy Act and/or described in its notice(s) or for a purpose that is compatible with those purposes; (ii) the organization where appropriate, enters into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the PII covered and specifically enumerate the purposes for which the PII may be used; (iii) the organization monitors, audits, and trains its staff on the authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII; and (iv) the organization evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required. | High | [Test: UL-2.1 - Information Sharing with Third Parties]  Not Entered |  |
| [E-# OR W-#] | Internal System Connections [NIST 800-53 w/ DHS 4300A CA-9] | [Test: CA-9.1 - Internal System Connections]  Not Entered | Failure to meet the internal system connection requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization authorizes internal connections of system components or classes of components to the information system; and, (ii) the organization documents, for each internal connection, the interface characteristics, security requirements, and the nature of the information communicated. | High | [Test: CA-9.1 - Internal System Connections]  Not Entered |  |
| [E-# OR W-#] | Security Awareness and Training Policy and Procedures [NIST 800-53 w/ DHS 4300A AT-1] | [Test: AT-1.1 - Security Awareness and Training Policy and Procedures]  Not Entered  [Test: AT-1.2 - Security Awareness and Training Policy and Procedures]  Not Entered | Failure to meet the requirements for security awareness and training policy and procedures indicated below could result in the ignorance of basic security practices, which could be taken advantage of by would-be attackers seeking to break into the information system of the organization through several foot-printing methods including, but not limited to, phishing and social engineering:  (i) the organization develops and formally documents security awareness and training policy; (ii) the organization security awareness and training policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; and * coordination among organizational entities, and compliance;   (iii) the organization disseminates formal documented security awareness and training policy to elements within the organization having associated security awareness and training roles and responsibilities; (iv) the organization develops and formally documents security awareness and training procedures; (v) the organization security awareness and training procedures facilitate implementation of the security awareness and training policy and associated security awareness and training controls; and (vi) the organization disseminates formal documented security awareness and training procedures to elements within the organization having associated security awareness and training roles and responsibilities.  Failure to meet the requirements for security awareness and training policy and procedures indicated below could result in unsuitable and inadequate security awareness and training policy and procedures, which could lead to the organization's personnel's incomplete knowledge of the policy and procedures and their extent:  (i) the organization defines the frequency of security awareness and training policy reviews/updates; (ii) the organization reviews/updates security awareness and training policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of security awareness and training procedure reviews/updates; and (iv) the organization reviews/updates security awareness and training procedures in accordance with organization-defined frequency. | High | [Test: AT-1.1 - Security Awareness and Training Policy and Procedures]  Not Entered  [Test: AT-1.2 - Security Awareness and Training Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | System and Services Acquisition Policy and Procedures [NIST 800-53 w/ DHS 4300A SA-1] | [Test: SA-1.1 - System and Services Acquisition Policy and Procedures]  Not Entered  [Test: SA-1.2 - System and Services Acquisition Policy and Procedures]  Not Entered | Failure to meet the system and services acquisition policy and procedures requirements listed below could result in the acquisition of a system/service that would expose the organization to various threats and exploits, which could cause the loss of critical mission/business assets or the disruption of organization operations, functions and services:  (i) the organization develops and formally documents system services and acquisition policy; (ii) the organization system services and acquisition policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented system services and acquisition policy to elements within the organization having associated system services and acquisition roles and responsibilities; (iv) the organization develops and formally documents system services and acquisition procedures; (v) the organization system services and acquisition procedures facilitate implementation of the system and services acquisition policy and associated system services and acquisition controls; and (vi) the organization disseminates formal documented system services and acquisition procedures to elements within the organization having associated system services and acquisition roles and responsibilities.  Failure to meet the system and services acquisition policy and procedures requirements listed below could result in the ineffective and incomplete acquisition of a system/service policy/procedure that would expose the organization to various threats and exploits, which could cause the loss of critical mission/business assets or the disruption of organization operations, functions and services:  (i) the organization defines the frequency of system services and acquisition policy reviews/updates; (ii) the organization reviews/updates system services and acquisition policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of system services and acquisition procedure reviews/updates; (iv) the organization reviews/updates system services and acquisition procedures in accordance with organization-defined frequency. | High | [Test: SA-1.1 - System and Services Acquisition Policy and Procedures]  Not Entered  [Test: SA-1.2 - System and Services Acquisition Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Physical and Environmental Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A PE-1] | [Test: PE-1.1 - Physical and Environmental Protection Policy and Procedures]  Not Entered  [Test: PE-1.2 - Physical and Environmental Protection Policy and Procedures]  Not Entered | Failure to meet the physical and environmental protection policy and procedures requirements indicated below could result in ineffective physical/environmental protection policy causing the lack of personnel/employee awareness on physical and environmental threats, which leaves the system and data more exposed and more susceptible to vulnerabilities:  (i) the organization defines the frequency of physical and environmental protection policy reviews/updates; (ii) the organization reviews/updates physical and environmental protection policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of physical and environmental protection procedure reviews/updates; (iv) the organization reviews/updates physical and environmental protection procedures in accordance with organization-defined frequency.  Failure to meet the physical and environmental protection policy and procedures requirements listed below could result in the lack of personnel/employee awareness on physical and environmental threats, which leaves the system and data more exposed and more susceptible to vulnerabilities:  (i) the organization develops and formally documents physical and environmental protection policy; (ii) the organization physical and environmental protection policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented physical and environmental protection policy to elements within the organization having associated physical and environmental protection roles and responsibilities; (iv) the organization develops and formally documents physical and environmental protection procedures; (v) the organization physical and environmental protection procedures facilitate implementation of the physical and environmental protection policy and associated physical and environmental protection controls; and (vi) the organization disseminates formal documented physical and environmental protection procedures to elements within the organization having associated physical and environmental protection roles and responsibilities. | High | [Test: PE-1.1 - Physical and Environmental Protection Policy and Procedures]  Not Entered  [Test: PE-1.2 - Physical and Environmental Protection Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Incident Response Training [NIST 800-53 w/ DHS 4300A IR-2] | [Test: IR-2.1 - Incident Response Training]  Not Entered | Failure to meet the incident response training requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system; (ii) the organization provides incident response training to personnel with incident response roles and responsibilities with respect to the information system; (iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities; (iv) the organization defines the frequency of refresher incident response training; and  (v) the organization provides refresher incident response training in accordance with the organization-defined frequency. | High | [Test: IR-2.1 - Incident Response Training]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6] | [Test: CM-6.1 - Configuration Settings]  Not Entered | Failure to meet the requirements for configuration settings listed below could lead to the compromise of the system or of the data in the system:  (i) the organization defines security configuration checklists to be used to establish and document mandatory configuration settings for the information system technology products employed; (ii) the organization-defined security configuration checklists reflect the most restrictive mode consistent with operational requirements; (iii) the organization establishes and documents mandatory configuration settings for information technology products employed within the information system using organization-defined security configuration checklists; (iv) the organization implements the security configuration settings; (v) the organization identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and (vi) the organization monitors and controls changes to the configuration settings in accordance with organizational policies and procedures. | High | [Test: CM-6.1 - Configuration Settings]  Not Entered |  |
| [E-# OR W-#] | Privacy Awareness and Training [NIST 800-53 w/ DHS 4300A PRIV-AR-5] | [Test: AR-5.1 - Privacy Awareness and Training]  Not Entered | Failure to meet the privacy awareness training requirements listed below could affect the readiness of personnel to respond to unexpected attacks and intrusion:  (i) the organization develops, implements, and updates a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures; (ii) the organization administers the following privacy privacy training at least annually:   * basic privacy training * targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII   (iii) the organization ensures that personnel certify (manually or electronically) acceptance of responsibilities for privacy requirements at least annually. | High | [Test: AR-5.1 - Privacy Awareness and Training]  Not Entered |  |
| [E-# OR W-#] | Dissemination of Privacy Program Information [NIST 800-53 w/ DHS 4300A PRIV-TR-3] | [Test: TR-3.1 - Dissemination of Privacy Program Information]  Not Entered | Failure to meet the privacy program information dissemination requirements listed below increases the risk to unauthorized disclosure of personally identifiable information:  (i) the organization ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO); and (ii) the organization ensures that its privacy practices are publicly available through organizational Web sites or otherwise. | High | [Test: TR-3.1 - Dissemination of Privacy Program Information]  Not Entered |  |
| [E-# OR W-#] | Redress [NIST 800-53 w/ DHS 4300A PRIV-IP-3] | [Test: IP-3.1 - Redress]  Not Entered | Failure to meet the redress requirements listed below increases could allow unauthorized individuals to view privacy information and disclose them without consent to other individuals:  (i) the organization provides a process for individuals to have inaccurate personally identifiable information (PII) maintained by the organization corrected or amended, as appropriate; and (ii) the organization establishes a process for disseminating corrections or amendments of the PII to other authorized users of the PII, such as external information-sharing partners and, where feasible and appropriate, notifies affected individuals that their information has been corrected or amended. | High | [Test: IP-3.1 - Redress]  Not Entered |  |
| [E-# OR W-#] | Threat Awareness Program [NIST 800-53 w/ DHS 4300A PM-16] | [Test: PM-16.1 - Threat Awareness Program]  Not Entered | Failure to ensure that the organization implements a threat awareness program that includes a cross organization information-sharing capability could result in the ignorance of basic security practices, which could be taken advantage of by would-be attackers seeking to break into the information system of the organization through several foot-printing methods including, but not limited to, phishing and social engineering. | High | [Test: PM-16.1 - Threat Awareness Program]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7] | [Test: CM-7.1 - Least Functionality]  Not Entered | Failure to meet the requirements for least functionality listed below could lead to the compromise of the system or of the data in the system:  (i) the organization defines for the information system prohibited or restricted:   * functions; * ports; * protocols; and * services;   (ii) the organization configures the information system to provide only essential capabilities; and (iii) the organization configures the information system to specifically prohibit or restrict the use of organization-defined:   * functions; * ports; * protocols; and/or * services. | High | [Test: CM-7.1 - Least Functionality]  Not Entered |  |
| [E-# OR W-#] | Security Assessments [NIST 800-53 w/ DHS 4300A CA-2] | [Test: CA-2.1 - Security Assessments]  Not Entered | Failure to meet the security assessments requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization develops a security assessment plan for the information system; and, (ii) the security assessment plan describes the scope of the assessment including:   * security controls and control enhancements under assessment; * assessment procedures to be used to determine security control effectiveness; and, * assessment environment, assessment team, and assessment roles and responsibilities. | High | [Test: CA-2.1 - Security Assessments]  Not Entered |  |
| [E-# OR W-#] | Privacy Monitoring and Auditing [NIST 800-53 w/ DHS 4300A PRIV-AR-4] | [Test: AR-4.1 - Privacy Monitoring and Auditing]  Not Entered | Failure to ensure that the organization employs a schedule to monitor and audit privacy controls and internal privacy policy could result in the inability of the organization to track any security incident, which could lead to other severe security threats. | High | [Test: AR-4.1 - Privacy Monitoring and Auditing]  Not Entered |  |
| [E-# OR W-#] | Incident Response Plan [NIST 800-53 w/ DHS 4300A IR-8] | [Test: IR-8.1 - Incident Response Plan]  Not Entered  [Test: IR-8.2 - Incident Response Plan]  Not Entered | Failure to meet the incident response plan requirements included below could prevent the immediate restoration of the system into its stable working state should an attack occur:   * provides the organization with a roadmap for implementing its incident response capability; * describes the structure and organization of the incident response capability; * provides a high-level approach for how the incident response capability fits into the overall organization; * meets the unique requirements of the organization, which relate to mission, size, structure, and functions; * defines reportable incidents; * provides metrics for measuring the incident response capability within the organization; * defines the resources and management support needed to effectively maintain and mature an incident response capability; and * is reviewed and approved by designated officials within the organization.   Failure to meet the incident response plan requirements listed below could prevent the immediate restoration of the system into its stable working state should an attack occur:  (i) the organization defines, in the incident response plan, incident response personnel (identified by name and/or role) and organizational elements; (ii) the organization distributes copies of the incident response plan to incident response personnel and organizational elements identified in the plan; (iii) the organization defines, in the incident response plan, the frequency to review the plan; (iv) the organization reviews the incident response plan in accordance with the organization-defined frequency; (v) the organization revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and (vi) the organization communicates incident response plan changes to incident response personnel and organizational elements identified in the plan. | High | [Test: IR-8.1 - Incident Response Plan]  Not Entered  [Test: IR-8.2 - Incident Response Plan]  Not Entered |  |
| [E-# OR W-#] | Audit Events [NIST 800-53 w/ DHS 4300A AU-2] | [Test: AU-2.1 - Audit Events]  Not Entered | Failure to meet the requirements for auditable events listed below could result in the failure of the audit process and inaccurate or incomplete system audit reports:  (i) the organization defines the list of events the information system must be capable of auditing; (ii) the organization determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the organization-defined list of auditable events; (iii) the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events; (iv) the organization provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; (v) the organization defines the subset of auditable events defined in (i) that are to be audited within the information system and the frequency of (or situation requiring) auditing for each identified event; and (vi) the organization determines, based on current threat information and ongoing assessment of risk, the subset of auditable events defined in (i) to be audited within the information system, and the frequency of (or situation requiring) auditing for each identified event. | High | [Test: AU-2.1 - Audit Events]  Not Entered |  |
| [E-# OR W-#] | Information Security Measures of Performance [NIST 800-53 w/ DHS 4300A PM-6] | [Test: PM-6.1 - Information Security Measures of Performance]  Not Entered | Failure to meet the information security measures of performance requirements listed below could risk the exposure of essential information compromising the confidentiality, integrity and availability of the system:  (i) the organization develops an inventory of its information systems; and (ii) the organization maintains an inventory of its information systems. | High | [Test: PM-6.1 - Information Security Measures of Performance]  Not Entered |  |
| [E-# OR W-#] | Access Agreements [NIST 800-53 w/ DHS 4300A PS-6] | [Test: PS-6.1 - Access Agreements]  Not Entered | Failure to meet access agreements requirements indicated below could lead to disclosure of greater amount of information:  (i) the organization develops and documents access agreements for organizational information systems;  (ii) the organization define the frequency of the access agreements reviews and updates; and  (iii) the organization ensures that individuals requiring access to organizational information and information systems:   * sign appropriate access agreements prior to being granted access; and * re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or organization-defined frequency. | High | [Test: PS-6.1 - Access Agreements]  Not Entered |  |
| [E-# OR W-#] | Incident Monitoring [NIST 800-53 w/ DHS 4300A IR-5] | [Test: IR-5.1 - Incident Monitoring]  Not Entered | Failure of the organization to track and document information system security incidents on an ongoing basis could lead to loss of system integrity. | High | [Test: IR-5.1 - Incident Monitoring]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7] | [Test: SC-7.1 - Boundary Protection]  Not Entered | Failure to meet the requirements for boundary protection listed below could lead to information disclosure:  (i) the information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; (ii) the information system implements subnetworks for publicly accessible system components that are physically or logically separated from internal organizational networks; and (iii) the information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture. | High | [Test: SC-7.1 - Boundary Protection]  Not Entered |  |
| [E-# OR W-#] | Privacy Impact and Risk Assessment [NIST 800-53 w/ DHS 4300A PRIV-AR-2] | [Test: AR-2.1 - Privacy Impact and Risk Assessment]  Not Entered | Failure to meet the privacy impact and risk assessment requirements listed below could lead eventually to the loss of personally identifiable information and other mission/business assets or to the disruption of other organization operations, functions and services:  (i) the organization documents and implements a privacy risk management process that assesses privacy risk to individuals resulting from the collection, sharing, storing, transmitting, use, and disposal of personally identifiable information (PII); and, (ii) the organization conducts Privacy Impact Assessments (PIAs) for information systems, programs, or other activities that pose a privacy risk in accordance with applicable law, OMB policy, or any existing organizational policies and procedures. | High | [Test: AR-2.1 - Privacy Impact and Risk Assessment]  Not Entered |  |
| [E-# OR W-#] | Information System Recovery and Reconstitution [NIST 800-53 w/ DHS 4300A CP-10] | [Test: CP-10.1 - Information System Recovery and Reconstitution]  Not Entered | Failure of the organization to provide and apply mechanisms and procedures for recovery and reconstitution of the information system to known secure state after disruption or failure could result in the loss of system integrity or stability, which could lead to the disruption of critical mission/business functions, operations, and processes. | High | [Test: CP-10.1 - Information System Recovery and Reconstitution]  Not Entered |  |
| [E-# OR W-#] | Flaw Remediation [NIST 800-53 w/ DHS 4300A SI-2] | [Test: SI-2.1 - Flaw Remediation]  Not Entered | Failure to meet the requirements for flaw remediation listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization identifies, reports, and corrects information system flaws; (ii) the organization tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; (iii) the organization installs security-relevant software and firmware updates within organization-defined time period of the release of the updates; and (iv) the organization incorporates flaw remediation into the organizational configuration management process. | High | [Test: SI-2.1 - Flaw Remediation]  Not Entered |  |
| [E-# OR W-#] | Incident Response Assistance [NIST 800-53 w/ DHS 4300A IR-7] | [Test: IR-7.1 - Incident Response Assistance]  Not Entered | Failure to meet the requirements for incident reporting listed below could lead to the compromise of the system or the misuse of data being processed, transported, or stored inside the system:  (i) the organization provides an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents; and (ii) the incident response support resource is an integral part of the organization's incident response capability. | High | [Test: IR-7.1 - Incident Response Assistance]  Not Entered |  |
| [E-# OR W-#] | Physical Access Authorizations [NIST 800-53 w/ DHS 4300A PE-2] | [Test: PE-2.1 - Physical Access Authorizations]  Not Entered  [Test: PE-2.2 - Physical Access Authorizations]  Not Entered | Failure to meet the requirements for physical access authorizations listed below could lead to the compromise of the system or of the data in the system:  (i) the organization identifies areas within the facility that are publicly accessible; (ii) the organization develops and keeps current lists of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and (iii) the organization issues authorization credentials (e.g., badges, identification cards, smart cards).  Failure to meet the requirements for physical access authorizations listed below could result in the loss of tangible assets or resources:  (i) the organization defines the frequency for review and approval of the physical access list and authorization credentials for the facility; (ii) organization reviews and approves the access list and authorization credentials in accordance with the organization-defined frequency; and (iii) the organization removes from the access list personnel no longer requiring access. | High | [Test: PE-2.1 - Physical Access Authorizations]  Not Entered  [Test: PE-2.2 - Physical Access Authorizations]  Not Entered |  |
| [E-# OR W-#] | Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19] | [Test: AC-19.1 - Access Control for Mobile Devices]  Not Entered | Failure to meet the requirements for access control for portable and mobile devices listed below could result in the failure of the audit process:  (i) the organization establishes usage restrictions and implementation guidance for organization-controlled portable and mobile devices; and, (ii) the organization authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems; | High | [Test: AC-19.1 - Access Control for Mobile Devices]  Not Entered |  |
| [E-# OR W-#] | Contingency Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A CP-1] | [Test: CP-1.1 - Contingency Planning Policy and Procedures]  Not Entered  [Test: CP-1.2 - Contingency Planning Policy and Procedures]  Not Entered | Failure to meet the contingency planning policy and procedures requirements listed below could leave the organization unprepared for any incident when it occurs due to incomplete or inaccurate plan and procedures, which could lead to the compromise of the system or of the data in the system:  (i) the organization defines the frequency of contingency planning policy reviews/updates; (ii) the organization reviews/updates contingency planning policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of contingency planning procedure reviews/updates; and (iv) the organization reviews/updates contingency planning procedures in accordance with organization-defined frequency.  Failure to meet the contingency planning policy and procedures requirements listed below could leave the organization unprepared for any incident when it occurs, which could lead to the compromise of the system or of the data in the system:  (i) the organization develops and formally documents contingency planning policy; (ii) the organization contingency planning policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented contingency planning policy to elements within the organization having associated contingency planning roles and responsibilities; (iv) the organization develops and formally documents contingency planning procedures; (v) the organization contingency planning procedures facilitate implementation of the contingency planning policy and associated contingency planning controls; and (vi) the organization disseminates formal documented contingency planning procedures to elements within the organization having associated contingency planning roles and responsibilities. | High | [Test: CP-1.1 - Contingency Planning Policy and Procedures]  Not Entered  [Test: CP-1.2 - Contingency Planning Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Use of External Information Systems [NIST 800-53 w/ DHS 4300A AC-20] | [Test: AC-20.1 - Use of External Information Systems]  Not Entered | Failure of the organization to establish terms and conditions for authorized individuals to access the information system from an external information system that include the types of applications that can be accessed on the organizational information system from the external information system and the maximum FIPS 199 security category of information that can be processed, stored, and transmitted on the external information system could result in a weaker security posture enabling would-be attackers to launch attack vectors targeted at vulnerable machines in the information system and cause damage to the resources therein:  (i) the organization identifies individuals authorized to:   * access the information system from the external information systems; and * process, store, and/or transmit organization-controlled information using the external information systems; and   (ii) the organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:   * access the information system from the external information systems; and * process, store, and/or transmit organization-controlled information using the external information system. | High | [Test: AC-20.1 - Use of External Information Systems]  Not Entered |  |
| [E-# OR W-#] | Information System Documentation [NIST 800-53 w/ DHS 4300A SA-5] | [Test: SA-5.1 - Information System Documentation]  Not Entered | Failure to meet the requirements for information system documentation listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization obtains administrator documentation for the information system, system component, or information system service that describes:   * secure configuration, installation, and operation of the system, component, or service; * effective use and maintenance of security functions/mechanisms; and * known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;   (ii) the organization obtains user documentation for the information system, system component, or information system service that describes:   * user-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms; * methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; and * user responsibilities in maintaining the security of the system, component, or service;   (iii) the organization documents attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent and organization-defined actions in response; (iv) the organization protects documentation as required, in accordance with the risk management strategy; and (v) the organization distributes documentation to organization-defined personnel or roles. | High | [Test: SA-5.1 - Information System Documentation]  Not Entered |  |
| [E-# OR W-#] | USB Drive encryption [NIST 800-53 w/ DHS 4300A MP-7 (DHS-4.3.1.d)] | [Test: MP-7(DHS-4.3.1.d) - USB Drive encryption]  Not Entered | Failure to ensure that all USB drives use encryption in compliance with Section 5.5.1 of this Policy Directive could lead to the organization to face litigations because of offenses related to non-compliance. | High | [Test: MP-7(DHS-4.3.1.d) - USB Drive encryption]  Not Entered |  |
| [E-# OR W-#] | Inventory of Personally Identifiable Information [NIST 800-53 w/ DHS 4300A PRIV-SE-1] | [Test: SE-1.1 - Inventory of Personally Identifiable Information]  Not Entered | Failure to meet the PII inventory requirements listed below increases the risk to loss, unauthorized access, or disclosure of personally identifiable information:  (i) the organization establishes, maintains, and updates an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing personally identifiable information (PII); and (ii) the organization provides each update of the PII inventory to the CIO or information security official [Assignment: organization-defined frequency] to support the establishment of information security requirements for all new or modified information systems containing PII. | High | [Test: SE-1.1 - Inventory of Personally Identifiable Information]  Not Entered |  |
| [E-# OR W-#] | System Security Plan [NIST 800-53 w/ DHS 4300A PL-2] | [Test: PL-2.1 - System Security Plan]  Not Entered | Failure to meet the system security plan requirements listed below could lead to the compromise of the system or of the data in the system:  (i) develops a security plan for the information system that:   * is consistent with the organization’s enterprise architecture; * explicitly defines the authorization boundary for the system; * describes the operational context of the information system in terms of missions and business processes; * provides the security categorization of the information system including supporting rationale; * describes the operational environment for the information system and relationships with or connections to other information systems; * provides an overview of the security requirements for the system; * identifies any relevant overlays, if applicable; * describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and * is reviewed and approved by the authorizing official or designated representative prior to plan implementation;   (ii) distributes copies of the security plan and communicates subsequent changes to the plan to organization-defined personnel or roles; (iii) defines the frequency of reviews the security plan for the information system;   * updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and * protects the security plan from unauthorized disclosure and modification. | High | [Test: PL-2.1 - System Security Plan]  Not Entered |  |
| [E-# OR W-#] | Emergency Lighting [NIST 800-53 w/ DHS 4300A PE-12] | [Test: PE-12.1 - Emergency Lighting]  Not Entered | Failure to ensure that the organization employs and maintains automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility could lead to the compromise of the system or of the data in the system. | High | [Test: PE-12.1 - Emergency Lighting]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17] | [Test: AC-17.1 - Remote Access]  Not Entered | Failure of the organization to authorize, monitor, and control remote access to the information system for all allowed methods of remote access to include both establishment of the remote connection and subsequent user actions across that connection could enable attackers to effect a system breach and cause damage to resources therein:  (i) establishes usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and, (ii) authorizes remote access to the information system prior to allowing such connections. | High | [Test: AC-17.1 - Remote Access]  Not Entered |  |
| [E-# OR W-#] | System Maintenance Policy and Procedures [NIST 800-53 w/ DHS 4300A MA-1] | [Test: MA-1.1 - System Maintenance Policy and Procedures]  Not Entered  [Test: MA-1.2 - System Maintenance Policy and Procedures]  Not Entered | Failure to meet the system maintenance policy and procedures requirements indicated below could result in malfunctioning systems due to incomplete and ineffective maintenance procedures, which could lead eventually to the system losing its stability or its integrity:  (i) the organization defines the frequency of system maintenance policy reviews/updates; (ii) the organization reviews/updates system maintenance policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of system maintenance procedure reviews/updates; (iv) the organization reviews/updates system maintenance procedures in accordance with organization-defined frequency.  Failure to meet the system maintenance policy and procedures requirements indicated below could result in malfunctioning systems, which could lead eventually to the system losing its stability or its integrity:  (i) the organization develops and formally documents system maintenance policy; (ii) the organization system maintenance policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented system maintenance policy to elements within the organization having associated system maintenance roles and responsibilities; (iv) the organization develops and formally documents system maintenance procedures; (v) the organization system maintenance procedures facilitate implementation of the system maintenance policy and associated system maintenance controls; and (vi) the organization disseminates formal documented system maintenance procedures to elements within the organization having associated system maintenance roles and responsibilities. | High | [Test: MA-1.1 - System Maintenance Policy and Procedures]  Not Entered  [Test: MA-1.2 - System Maintenance Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Information Security Resources [NIST 800-53 w/ DHS 4300A PM-3] | [Test: PM-3.1 - Information Security Resources]  Not Entered | Failure to meet the information security resources requirements listed below could risk the exposure of essential information compromising the confidentiality, integrity and availability of the system:  (i) the organization ensures that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement; (ii) the organization employs a business case/Exhibit 300/Exhibit 53 to record the resources required; and (iii) the organization ensures that information security resources are available for expenditure as planned. | High | [Test: PM-3.1 - Information Security Resources]  Not Entered |  |
| [E-# OR W-#] | Security Authorization [NIST 800-53 w/ DHS 4300A CA-6] | [Test: CA-6.1 - Security Authorization]  Not Entered | Failure to meet the security authorization requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization assigns a senior-level executive or manager to the role of authorizing official for the information system; (ii) the authorizing official authorizes the information system for processing before commencing operations; (iii) the organization defines the frequency of security authorization updates; and (iv) the organization updates the security authorization in accordance with an organization-defined frequency. | High | [Test: CA-6.1 - Security Authorization]  Not Entered |  |
| [E-# OR W-#] | Risk Assessment [NIST 800-53 w/ DHS 4300A RA-3] | [Test: RA-3.1 - Risk Assessment]  Not Entered | Failure to meet the requirements for risk assessment listed below could result in weaker security posture, which could lead to unauthorized disclosure of more information:  (i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:   * access; * use; * disclosure; * disruption; * modification; or * destruction;   (ii) the organization defines the document in which risk assessment results are documented, selecting from the security plan, risk assessment report, or other organization-defined document; (iii) the organization defines the frequency updates of the risk assessment or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system. | High | [Test: RA-3.1 - Risk Assessment]  Not Entered |  |
| [E-# OR W-#] | Audit Generation [NIST 800-53 w/ DHS 4300A AU-12] | [Test: AU-12.1 - Audit Generation]  Not Entered | Failure to meet the audit generation requirements listed below could result in the loss of the generated audit data, which could render an audit or forensic investigation efforts useless:  (i) the organization defines the information system components that provide audit record generation capability for the list of auditable events defined in AU-2; (ii) the information system provides audit record generation capability, at organization-defined information system components, for the list of auditable events defined in AU-2; (iii) the information system allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and, (iv) the information system generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3. | High | [Test: AU-12.1 - Audit Generation]  Not Entered |  |
| [E-# OR W-#] | Incident Response Policy and Procedures [NIST 800-53 w/ DHS 4300A IR-1] | [Test: IR-1.1 - Incident Response Policy and Procedures]  Not Entered  [Test: IR-1.2 - Incident Response Policy and Procedures]  Not Entered | Failure to meet the incident response policy and procedures requirements listed below could result in ineffective and incomplete incidence response procedures, which could lead to the disruption of critical mission/business functions, operations, and processes:  (i) the organization defines the frequency of incident response policy reviews/updates; (ii) the organization reviews/updates incident response policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of incident response procedure reviews/updates; and (iv) the organization reviews/updates incident response procedures in accordance with organization-defined frequency.  Failure to meet the incident response policy and procedures requirements listed below could result in the inability of the key organization personnel to respond properly to an incident in a timely manner, which could lead to the disruption of critical mission/business functions, operations, and processes:   (i) the organization develops and formally documents incident response policy; (ii) the organization incident response policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented incident response policy to elements within the organization having associated incident response roles and responsibilities; (iv) the organization develops and formally documents incident response procedures; (v) the organization incident response procedures facilitate implementation of the incident response policy and associated incident response controls; and (vi) the organization disseminates formal documented incident response procedures to elements within the organization having associated incident response roles and responsibilities. | High | [Test: IR-1.1 - Incident Response Policy and Procedures]  Not Entered  [Test: IR-1.2 - Incident Response Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Data Quality [NIST 800-53 w/ DHS 4300A PRIV-DI-1] | [Test: DI-1.1 - Data Quality]  Not Entered | Failure to meet the data quality requirements listed below could lead to the compromise or unauthorized disclosure of personally identifiable information:  (i) confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information; (ii) collects PII directly from the individual to the greatest extent practicable; (iii) checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems in accordance with organization-defined frequency; and, (iv) issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. | High | [Test: DI-1.1 - Data Quality]  Not Entered |  |
| [E-# OR W-#] | Delivery and Removal [NIST 800-53 w/ DHS 4300A PE-16] | [Test: PE-16.1 - Delivery and Removal]  Not Entered | Failure to ensure that the organization authorizes, monitors, and controls organization-defined types of information system components entering and exiting the facility and maintains records of those items could result in a weak security stance of the organization due to malfunctioning hardware/firmware or unsafe software. | High | [Test: PE-16.1 - Delivery and Removal]  Not Entered |  |
| [E-# OR W-#] | Risk Management Strategy [NIST 800-53 w/ DHS 4300A PM-9] | [Test: PM-9.1 - Risk Management Strategy]  Not Entered | Failure to meet the risk management strategy requirements listed below could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; and (ii) the organization implements that strategy consistently across the organization. | High | [Test: PM-9.1 - Risk Management Strategy]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5] | [Test: IA-5.1 - Authenticator Management]  Not Entered | Failure to meet the authenticator management requirements listed below could result in the loss of system integrity:  (i) the organization defines the time period (by authenticator type) for changing/refreshing authenticators; and (ii) the organization manages information system authenticators for users and devices by:   * verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator; * establishing initial authenticator content for authenticators defined by the organization; * ensuring that authenticators have sufficient strength of mechanism for their intended use; * establishing and implementing administrative procedures for initial authenticator distribution; * establishing and implementing administrative procedures for lost/compromised or damaged authenticators; * establishing and implementing administrative procedures for revoking authenticators; * changing default content of authenticators upon information system installation; * establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if deemed to be appropriate by the organization); * changing/refreshing authenticators in accordance with the organization-defined time period by authenticator type; * protecting authenticator content from unauthorized disclosure and modification; and * requiring users to take, and having devices implement, specific measures to safeguard authenticators. | High | [Test: IA-5.1 - Authenticator Management]  Not Entered |  |
| [E-# OR W-#] | Testing, Training, and Monitoring [NIST 800-53 w/ DHS 4300A PM-14] | [Test: PM-14.1 - Testing, Training, and Monitoring]  Not Entered | Failure to meet the testing, training, and monitoring requirements indicated below could result in the ignorance of basic security practices, which could be taken advantage of by would-be attackers seeking to break into the information system of the organization through several foot-printing methods including, but not limited to, phishing and social engineering:  (i) the organization implements a process for ensuring that organizational plans for conducting security testing, training, and monitoring activities associated with organizational information systems:   * are developed and maintained; and * continue to be executed in a timely manner;   (ii) the organization reviews testing, training, and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | High | [Test: PM-14.1 - Testing, Training, and Monitoring]  Not Entered |  |
| [E-# OR W-#] | Software Usage Restrictions [NIST 800-53 w/ DHS 4300A CM-10] | [Test: CM-10.1 - Software Usage Restrictions]  Not Entered | Failure to meet the software usage restriction requirements listed below could weaken the overall security posture of the system:  (i) the organization uses software and associated documentation in accordance with contract agreements and copyright laws; (ii) the organization tracks the use of software and associated documentation protected by quantity licenses to control copying and distribution; and, (iii) the organization controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work. | High | [Test: CM-10.1 - Software Usage Restrictions]  Not Entered |  |
| [E-# OR W-#] | Purpose Specification [NIST 800-53 w/ DHS 4300A PRIV-AP-2] | [Test: AP-2.1 - Purpose Specification]  Not Entered | Failure to meet the privacy control requirements for collecting PIIs listed below could lead to unauthorized disclosure of personal identifiable information:  (i) the organization identifies the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and, (ii) the organization specifies in their notices the purpose(s) for which PII is collected. | High | [Test: AP-2.1 - Purpose Specification]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4] | [Test: PL-4.1 - Rules of Behavior]  Not Entered | Failure to meet the security plan update requirements listed below could leave the users unaware of the required behavior with regard to information usage, which could lead to the user inadvertently abusing the information system resources:  (i) the organization establishes the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage; (ii) the organization makes the rules available to all information system users; and (iii) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | High | [Test: PL-4.1 - Rules of Behavior]  Not Entered |  |
| [E-# OR W-#] | Security Alerts, Advisories, and Directives [NIST 800-53 w/ DHS 4300A SI-5] | [Test: SI-5.1 - Security Alerts, Advisories, and Directives]  Not Entered | Failure to meet the security alerts requirements listed below could result in a weak security stance of the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization receives information system security alerts, advisories, and directives from [Assignment: organization-defined external organizations] on an ongoing basis; (ii) the organization generates internal security alerts, advisories, and directives as deemed necessary; (iii) the organization disseminates security alerts, advisories, and directives to organization-defined personnel or roles, organization-defined elements within the organization, or organization-defined external organizations; and (iv) the organization implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance. | High | [Test: SI-5.1 - Security Alerts, Advisories, and Directives]  Not Entered |  |
| [E-# OR W-#] | Privacy Reporting [NIST 800-53 w/ DHS 4300A PRIV-AR-6] | [Test: AR-6.1 - Privacy Reporting]  Not Entered | Failure to meet the privacy reporting requirements listed below could lead to the compromise of the system or the misuse of PII or other classified information stored inside the system:  (i) the organization conducts internal and external privacy reporting. (ii) the organization submits privacy reports such as the following:   * annual Senior Agency Official for Privacy (SAOP) reports to OMB; * reports to Congress required by the Implementing Regulations of the 9/11 Commission Act; and, * other public reports required by specific statutory mandates or internal policies of organizations.   (iii) the organization develops, disseminates, and updates privacy reports to authorized personnel and other oversight bodies with responsibility for monitoring privacy program progress and compliance. | High | [Test: AR-6.1 - Privacy Reporting]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2] | [Test: CM-2.1 - Baseline Configuration]  Not Entered | Failure to meet the baseline configuration requirements listed below could result in a system that is not properly configured or with a weak security stance, which could lead to the compromise of data or the system itself:  (i) the organization develops and documents a baseline configuration of the information system and (ii) the organization maintains, under configuration control, a current baseline configuration of the information system. | High | [Test: CM-2.1 - Baseline Configuration]  Not Entered |  |
| [E-# OR W-#] | System Use Notification [NIST 800-53 w/ DHS 4300A AC-8] | [Test: AC-8.1 - System Use Notification]  Not Entered  [Test: AC-8.2 - System Use Notification]  Not Entered | Failure of the information system notification message to include topics such as the ones indicated below could further encourage an attacker to try and break into the system:  (i) the organization approves the information system use notification message or banner to be displayed by the information system before granting access to the system; (ii) the information system displays the approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that:   * users are accessing a U.S. Government information system; * system usage may be monitored, recorded, and subject to audit; * unauthorized use of the system is prohibited and subject to criminal and civil penalties; and * use of the system indicates consent to monitoring and recording; and   (iii) the information system retains the notification message or banner on the screen until the user takes explicit actions to log on to or further access the information system.  Failure to meet the system use notification requirements listed below could further encourage an attacker to try and break into the system due to low security policies:  (i) the information system (for publicly accessible systems) displays the system use information when appropriate, before granting further access; (ii) the information system (for publicly accessible systems) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) the information system (for publicly accessible systems) includes in the notice given to public users of the information system, a description of the authorized uses of the information system. | High | [Test: AC-8.1 - System Use Notification]  Not Entered  [Test: AC-8.2 - System Use Notification]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5] | [Test: RA-5.1 - Vulnerability Scanning]  Not Entered  [Test: RA-5.2 - Vulnerability Scanning]  Not Entered | Failure to meet the requirements for vulnerability scanning listed below could put the organization in weaker security posture that could result in unauthorized disclosure of information, greater compromise of the system, or to other more severe security threats against the organization:  (i) the organization defines the response times for remediating legitimate vulnerabilities in accordance with an organizational assessment of risk; (ii) the organization remediates legitimate vulnerabilities in accordance with organization-defined response times; and (iii) the organization shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).  Failure to meet the requirements for vulnerability scanning listed below could put the organization in weaker security posture that could result in unauthorized disclosure of information, greater compromise of the system, or to other more severe security threats against the organization:  (i) the organization defines:   * the frequency for conducting vulnerability scans on the information system and hosted applications and/or; * the organization-defined process for conducting random vulnerability scans on the information system and hosted applications;   (ii) the organization scans for vulnerabilities in the information system and hosted applications in accordance with the organization-defined frequency and/or the organization-defined process for random scans; (iii) the organization scans for vulnerabilities in the information system and hosted applications when new vulnerabilities potentially affecting the system/applications are identified and reported; (iv) the organization employs vulnerability scanning tools and techniques that use standards to promote interoperability among tools and automate parts of the vulnerability management process that focus on:   * enumerating platforms, software flaws, and improper configurations; * formatting/and making transparent checklists and test procedures; and * measuring vulnerability impact, and   (v) the organization analyzes vulnerability scan reports and results from security control assessments. | High | [Test: RA-5.1 - Vulnerability Scanning]  Not Entered  [Test: RA-5.2 - Vulnerability Scanning]  Not Entered |  |
| [E-# OR W-#] | Wireless Access [NIST 800-53 w/ DHS 4300A AC-18] | [Test: AC-18.1 - Wireless Access]  Not Entered | Failure to meet the wireless access restrictions requirements indicated below could result in a number of unmanaged and unauthorized wireless access to the information system:  (i) the organization establishes usage restrictions and implementation guidance for wireless access; (ii) the organization monitors for unauthorized wireless access to the information system; (iii) the organization authorizes wireless access to the information system prior to connection; and  (iv) the organization enforces requirements for wireless connections to the information system. | High | [Test: AC-18.1 - Wireless Access]  Not Entered |  |
| [E-# OR W-#] | Information Security Workforce [NIST 800-53 w/ DHS 4300A PM-13] | [Test: PM-13.1 - Information Security Workforce]  Not Entered | Failure to ensure that the organization establishes an information security workforce development and improvement program could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: PM-13.1 - Information Security Workforce]  Not Entered |  |
| [E-# OR W-#] | Access Control Policy and Procedures [NIST 800-53 w/ DHS 4300A AC-1] | [Test: AC-1.1 - Access Control Policy and Procedures]  Not Entered  [Test: AC-1.2 - Access Control Policy and Procedures]  Not Entered | Failure to meet the access control policy and procedures requirements listed below could result in a weaker organizational structure where the policy conflicts with the trust, accountabilities, entities, interests, and requirements of the organization, which could lead to a weaker security posture enabling prospecting intruders to take advantage of the probable confusion and conflict brought about by an inadequate access control policy:  (i) the organization defines the frequency of access control policy reviews/updates; (ii) the organization reviews/updates access control policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of access control procedure reviews/updates; and (iv) the organization reviews/updates access control procedures in accordance with organization-defined frequency.  Failure to meet the access control policy and procedures requirements listed below could result in a weaker security posture as a consequence of a failed audit process, the non-accountability of critical actions, and ignorance to the policy being implemented for the organization:  (i) the organization develops and formally documents access control policy; (ii) the organization access control policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented access control policy to elements within the organization having associated access control roles and responsibilities; (iv) the organization develops and formally documents access control procedures; (v) the organization access control procedures facilitate implementation of the access control policy and associated access controls; and (vi) the organization disseminates formal documented access control procedures to elements within the organization having associated access control roles and responsibilities. | High | [Test: AC-1.1 - Access Control Policy and Procedures]  Not Entered  [Test: AC-1.2 - Access Control Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1] | [Test: SC-1.1 - System and Communications Protection Policy and Procedures]  Not Entered  [Test: SC-1.2 - System and Communications Protection Policy and Procedures]  Not Entered | Failure to meet the system and communications protection requirements indicated below could result in unsafe and ineffective communication systems due to ineffective and incomplete communication protection policy, which could eventually lead to the loss of critical mission/business assets and information or to the disruption of organization operations, functions and services:  (i) the organization defines the frequency of system and communications protection policy reviews/updates; (ii) the organization reviews/updates system and communications protection policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of system and communications protection procedure reviews/updates; (iv) the organization reviews/updates system and communications protection procedures in accordance with organization-defined frequency.  Failure to meet the system and communications protection requirements indicated below could result in unsafe and ineffective communication systems, which could eventually lead to the loss of critical mission/business assets and information or to the disruption of organization operations, functions and services:  (i) the organization develops and documents system and communications protection policy and procedures; (ii) the organization disseminates system and communications protection policy and procedures to appropriate elements within the organization; (iii) responsible parties within the organization periodically review system and communications protection policy and procedures; and, (iv) the organization updates system and communications protection policy and procedures when organizational review indicates updates are required. | High | [Test: SC-1.1 - System and Communications Protection Policy and Procedures]  Not Entered  [Test: SC-1.2 - System and Communications Protection Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Malicious Code Protection [NIST 800-53 w/ DHS 4300A SI-3] | [Test: SI-3.1 - Malicious Code Protection]  Not Entered | Failure to meet the requirements for malicious code protection listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; (ii) the organization updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; (iii) the organization configures malicious code protection mechanisms to:   * perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at endpoint or network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and * Block malicious code, quarantine malicious code, send alert to administrator, or organization-defined action in response to malicious code detection; and   (iv) the organization addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system. | High | [Test: SI-3.1 - Malicious Code Protection]  Not Entered |  |
| [E-# OR W-#] | Individual Access [NIST 800-53 w/ DHS 4300A PRIV-IP-2] | [Test: IP-2.1 - Individual Access]  Not Entered | Failure to meet the individual access requirements listed below increases could allow unauthorized individuals to view privacy information and disclose them without consent to other individuals:  (i) provides individuals the ability to have access to their personally identifiable information (PII) maintained in its system(s) of records; (ii) publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of records; (iii) publishes access procedures in System of Records Notices (SORNs); and, (iv) adheres to Privacy Act requirements and OMB policies and guidance for the proper processing of Privacy Act requests. | High | [Test: IP-2.1 - Individual Access]  Not Entered |  |
| [E-# OR W-#] | Security Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A PL-1] | [Test: PL-1.1 - Security Planning Policy and Procedures]  Not Entered  [Test: PL-1.2 - Security Planning Policy and Procedures]  Not Entered | Failure to meet the security planning policy and procedures requirements listed below could result in the weak security stance of the organization due to ineffective and incomplete security planning policy and procedures:  (i) the organization defines the frequency of security planning policy reviews/updates; (ii) the organization reviews/updates security planning policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of security planning procedure reviews/updates; (iv) the organization reviews/updates security planning procedures in accordance with organization-defined frequency.  Failure to meet the security planning policy and procedures requirements listed below could result in the weak security stance of the organization due to the lack of awareness on the security planning policy and procedures:  (i) the organization develops and formally documents security planning policy; (ii) the organization security planning policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented security planning policy to elements within the organization having associated security planning roles and responsibilities; (iv) the organization develops and formally documents security planning procedures; (v) the organization security planning procedures facilitate implementation of the security planning policy and associated security planning controls; and (vi) the organization disseminates formal documented security planning procedures to elements within the organization having associated security planning roles and responsibilities. | High | [Test: PL-1.1 - Security Planning Policy and Procedures]  Not Entered  [Test: PL-1.2 - Security Planning Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Authenticator Feedback [NIST 800-53 w/ DHS 4300A IA-6] | [Test: IA-6.1 - Authenticator Feedback]  Not Entered | Failure of the information system to obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals could lead to the compromise of the system or of the data in the system. | High | [Test: IA-6.1 - Authenticator Feedback]  Not Entered |  |
| [E-# OR W-#] | Information System Inventory [NIST 800-53 w/ DHS 4300A PM-5] | [Test: PM-5.1 - Information System Inventory]  Not Entered | Failure to ensure that the organization develops and maintains an inventory of its information systems could risk the exposure of essential information compromising the confidentiality, integrity and availability of the system. | High | [Test: PM-5.1 - Information System Inventory]  Not Entered |  |
| [E-# OR W-#] | Media Access [NIST 800-53 w/ DHS 4300A MP-2] | [Test: MP-2.1 - Media Access]  Not Entered | Failure to ensure that the organization defines digital and non-digital media requiring restricted access to authorized individuals could lead to the compromise of the system or of the data in the system. | High | [Test: MP-2.1 - Media Access]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2] | [Test: AC-2.1 - Account Management]  Not Entered | Failure to meet the account management requirements listed below could enable an intruder to gain access to a system account through social engineering or other methods and elevate the account's rights to a higher privileged account to try and penetrate the system and cause intentional or unintentional damage:  (i) the organization identifies information system accounts to support organizational missions/business functions; (ii) the organization assigns account managers for information system accounts; (iii) the organization establishes conditions for group and role membership; (iv) the organization specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account; (v) the organization requires approvals by organization-defined personnel or roles for requests to create information system accounts; (vi) the organization creates, enables, modifies, disables, and removes information system accounts; (vii) the organization authorizes, and monitors the use of, information system accounts; (viii) the organization notifies account managers:   * When accounts are no longer required; * When users are terminated or transferred; and, * When individual information system usage or need-to-know changes;   (ix) the organization authorizes access to the information system based on:   * A valid access authorization; * Intended system usage; and, * Other attributes as required by the organization or associated missions/business functions;   (x) the organization reviews accounts for compliance with account management requirements in accordance with organization-defined frequency; and, (xi) the organization establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. | High | [Test: AC-2.1 - Account Management]  Not Entered |  |
| [E-# OR W-#] | Data Integrity and Data Integrity Board [NIST 800-53 w/ DHS 4300A PRIV-DI-2] | [Test: DI-2.1 - Data Integrity and Data Integrity Board]  Not Entered | Failure to meet the requirements for data integrity and data integrity board listed below could result in the non-accountability of critical actions, and ignorance to the policy being implemented for the organization:  (i) the organization documents processes to ensure the integrity of personally identifiable information (PII) through existing security controls; and, (ii) the organization establishes a Data Integrity Board when appropriate to oversee organizational Computer Matching Agreements123 and to ensure that those agreements comply with the computer matching provisions of the Privacy Act. | High | [Test: DI-2.1 - Data Integrity and Data Integrity Board]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12] | [Test: SC-12.1 - Cryptographic Key Establishment and Management]  Not Entered | Failure to ensure that the organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with organization-defined requirements for key generation, distribution, storage, access, and destruction could lead to the disclosure of critical mission/business information/data. | High | [Test: SC-12.1 - Cryptographic Key Establishment and Management]  Not Entered |  |
| [E-# OR W-#] | Data Retention and Disposal [NIST 800-53 w/ DHS 4300A PRIV-DM-2] | [Test: DM-2.1 - Data Retention and Disposal]  Not Entered | Failure to meet the data retention and disposal requirements listed below could result in the disclosure of critical and sensitive personally identifiable information:  (i) the organization identifies the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection; (ii) the organization limits the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and, (iii) the organization conducts an initial evaluation of PII holdings and establishes and follows a schedule for regularly reviewing those holdings , at least annually, to ensure that only PII identified in the notice is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose. | High | [Test: DM-2.1 - Data Retention and Disposal]  Not Entered |  |
| [E-# OR W-#] | Information System Monitoring [NIST 800-53 w/ DHS 4300A SI-4] | [Test: SI-4.1 - Information System Monitoring]  Not Entered | Failure to meet the requirements for information system monitoring tools and techniques listed below could result in the inability to detect any attack on, intrusion of or malicious/abusive use of the information system enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization monitors the information system to detect:   * Attacks and indicators of potential attacks in accordance with [Assignment: organization-defined monitoring objectives]; and * Unauthorized local, network, and remote connections;   (ii) the organization identifies unauthorized use of the information system through [Assignment: organization-defined techniques and methods]; (iii) the organization deploys monitoring devices:   * strategically within the information system to collect organization-determined essential information; and * at ad hoc locations within the system to track specific types of transactions of interest to the organization;   (iv) the organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; (v) the organization heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; and (vi) the organization obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations. | High | [Test: SI-4.1 - Information System Monitoring]  Not Entered |  |
| [E-# OR W-#] | Complaint Management [NIST 800-53 w/ DHS 4300A PRIV-IP-4] | [Test: IP-4.1 - Complaint Management]  Not Entered | Failure to ensure that the organization implements complaints management procedures to organizational privacy practices could lead PII issues and concerns unattended, which increases the risk to unauthorized disclosure of privacy information. | High | [Test: IP-4.1 - Complaint Management]  Not Entered |  |
| [E-# OR W-#] | Plan of Action and Milestones Process [NIST 800-53 w/ DHS 4300A PM-4] | [Test: PM-4.1 - Plan of Action and Milestones Process]  Not Entered | Failure to meet the plan of action and milestones process requirements listed below could risk the exposure of essential information compromising the confidentiality, integrity and availability of the system:  (i) the organization implements a process for ensuring that plans of action and milestones for the security program and associated organizational information systems:   * are developed and maintained; * document the remedial information security actions to adequately respond to risk to organizational operations and assets, individuals, other organizations, and the Nation; and * are reported in accordance with OMB FISMA reporting requirements.   (ii) the organization reviews plans of action and milestones for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions. | High | [Test: PM-4.1 - Plan of Action and Milestones Process]  Not Entered |  |
| [E-# OR W-#] | Minimization of PII Used in Testing, Training, and Research [NIST 800-53 w/ DHS 4300A PRIV-DM-3] | [Test: DM-3.1 - Minimization of PII Used in Testing, Training, and Research]  Not Entered | Failure to meet the PII testing, research, and training requirements listed below increases risk of unauthorized disclosure or misuse of the information:  (i) the organization develops policies and procedures that minimize the use of personally identifiable information (PII) for testing, training, and research; and, (ii) the organization implements controls to protect PII used for testing, training, and research. | High | [Test: DM-3.1 - Minimization of PII Used in Testing, Training, and Research]  Not Entered |  |
| [E-# OR W-#] | Configuration Management Policy and Procedures [NIST 800-53 w/ DHS 4300A CM-1] | [Test: CM-1.1 - Configuration Management Policy and Procedures]  Not Entered  [Test: CM-1.2 - Configuration Management Policy and Procedures]  Not Entered | Failure to meet the configuration management policy and procedures requirements indicated below could result in a weak security stance of the organization due to confusing, non-standard and incomplete policy and procedures:  (i) the organization defines the frequency of configuration management policy reviews/updates; (ii) the organization reviews/updates configuration management policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of configuration management procedure reviews/updates; and (iv) the organization reviews/updates configuration management procedures in accordance with organization-defined frequency.  Failure to meet the configuration management policy and procedures requirements listed below could risk the integrity and stability of the system:  (i) the organization develops and formally documents configuration management policy; (ii) the organization configuration management policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented configuration management policy to elements within the organization having associated configuration management roles and responsibilities; (iv) the organization develops and formally documents configuration management procedures; (v) the organization configuration management procedures facilitate implementation of the configuration management policy and associated configuration management controls; and (vi) the organization disseminates formal documented configuration management procedures to elements within the organization having associated configuration management roles and responsibilities. | High | [Test: CM-1.1 - Configuration Management Policy and Procedures]  Not Entered  [Test: CM-1.2 - Configuration Management Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Plan of Action and Milestones [NIST 800-53 w/ DHS 4300A CA-5] | [Test: CA-5.1 - Plan of Action and Milestones]  Not Entered | Failure to meet the plan of action and milestones requirements listed below exposes the system to security threats due to security holes that could have been patched in a timely manner, which could eventually lead to the compromise of the system or of the data in the system:  (i) the organization develops a plan of action and milestones for the information system; (ii) the plan of action and milestones documents the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; (iii) the organization defines the frequency of plan of action and milestone updates; and (iv) the organization updates the plan of action and milestones at an organization-defined frequency with findings from:   * security controls assessments; * security impact analyses; and * continuous monitoring activities. | High | [Test: CA-5.1 - Plan of Action and Milestones]  Not Entered |  |
| [E-# OR W-#] | Content of Audit Records [NIST 800-53 w/ DHS 4300A AU-3] | [Test: AU-3.1 - Content of Audit Records]  Not Entered | Failure to meet requirements for content of audit records indicated below could result in incomplete data critical to the success of a forensic process:   * what type of event occurred; * when (date and time) the event occurred; * where the event occurred; * the source of the event; * the outcome (success or failure) of the event; and, * the identity of any user/subject associated with the event. | High | [Test: AU-3.1 - Content of Audit Records]  Not Entered |  |
| [E-# OR W-#] | Security Training Records [NIST 800-53 w/ DHS 4300A AT-4] | [Test: AT-4.1 - Security Training Records]  Not Entered | Failure to meet the security training record requirements listed below could result in the dissemination of unsuitable, unauthorized or erroneous security-related content in the training:  (i) the organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; (ii) the organization defines the time period for retaining individual training records; and, (iii) the organization retains individual training records in accordance with the organization-defined time period. | High | [Test: AT-4.1 - Security Training Records]  Not Entered |  |
| [E-# OR W-#] | Protection of Sensitive Paper and Electronic Outputs [NIST 800-53 w/ DHS 4300A MP-7 (DHS-4.3.1.f)] | [Test: MP-7(DHS-4.3.1.f) - Protection of Sensitive Paper and Electronic Outputs]  Not Entered | Failure of the components to follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected could result in the disclosure of critical and sensitive mission/business information that may have been contained in the media. | High | [Test: MP-7(DHS-4.3.1.f) - Protection of Sensitive Paper and Electronic Outputs]  Not Entered |  |
| [E-# OR W-#] | User-Installed Software [NIST 800-53 w/ DHS 4300A CM-11] | [Test: CM-11.1 - User-Installed Software]  Not Entered | Failure to meet the user-Installed software requirements listed below could weaken the overall security posture of the system:  (i) the organization establishes organization-defined policies governing the installation of software by users; (ii) the organization enforces software installation policies through organization-defined methods; and, (iii) the organization monitors policy compliance at an organization-defined frequency. | High | [Test: CM-11.1 - User-Installed Software]  Not Entered |  |
| [E-# OR W-#] | Media Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A MP-1] | [Test: MP-1.1 - Media Protection Policy and Procedures]  Not Entered  [Test: MP-1.2 - Media Protection Policy and Procedures]  Not Entered | Failure to meet the media protection policy and procedures requirements indicated below could result in an ineffective media protection, which could eventually lead to the organization losing critical mission/business assets in the form of unauthorized or unintentional disclosure of information:  (i) the organization defines the frequency of media protection policy reviews/updates; (ii) the organization reviews/updates media protection policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of media protection procedure reviews/updates; (iv) the organization reviews/updates media protection procedures in accordance with organization-defined frequency.  Failure to meet the media protection policy and procedures requirements indicated below could result in the personnel or employee being unaware of the proper media protection or its extent, which could eventually lead to the organization losing critical mission/business assets in the form of unauthorized or unintentional disclosure of information:  (i) the organization develops and formally documents media protection policy; (ii) the organization media protection policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented media protection policy to elements within the organization having associated media protection roles and responsibilities; (iv) the organization develops and formally documents media protection procedures; (v) the organization media protection procedures facilitate implementation of the media protection policy and associated media protection controls; and (vi) the organization disseminates formal documented media protection procedures to elements within the organization having associated media protection roles and responsibilities. | High | [Test: MP-1.1 - Media Protection Policy and Procedures]  Not Entered  [Test: MP-1.2 - Media Protection Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Third-Party Personnel Security [NIST 800-53 w/ DHS 4300A PS-7] | [Test: PS-7.1 - Third-Party Personnel Security]  Not Entered | Failure to meet the third-party personnel security requirements indicated below could lead to disclosure of information through the third-party products or applications:  (i) the organization establishes personnel security requirements including security roles and responsibilities for third-party providers;  (ii) the organization requires third-party providers to comply with personnel security policies and procedures established by the organization;  (iii) the organization documents personnel security requirements;  (iv) the organization requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational credentials and/or badges, or who have information system privileges within organization-defined time period; and  (v) the organization monitors provider compliance. | High | [Test: PS-7.1 - Third-Party Personnel Security]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2] | [Test: IA-2.1 - Identification and Authentication (Organizational Users)]  Not Entered | Failure to ensure that the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users) could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data. | High | [Test: IA-2.1 - Identification and Authentication (Organizational Users)]  Not Entered |  |
| [E-# OR W-#] | Time Stamps [NIST 800-53 w/ DHS 4300A AU-8] | [Test: AU-8.1 - Time Stamps]  Not Entered | Failure to meet the time stamp requirements listed below could lead to compromise of the system or of the data in the system:  (i) the information system uses internal system clocks to generate time stamps for audit records; (ii) the information system generates time in the time stamps that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT); and, (iii) the organization defines different time granularities for different system components. | High | [Test: AU-8.1 - Time Stamps]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Module Authentication [NIST 800-53 w/ DHS 4300A IA-7] | [Test: IA-7.1 - Cryptographic Module Authentication]  Not Entered | Failure of the information system to employ authentication methods that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module (for non-national security systems, the cryptographic requirements are defined by FOPS 140-2, as amended) could lead to the compromise of the system or of the data in the system. | High | [Test: IA-7.1 - Cryptographic Module Authentication]  Not Entered |  |
| [E-# OR W-#] | Security Categorization [NIST 800-53 w/ DHS 4300A RA-2] | [Test: RA-2.1 - Security Categorization]  Not Entered | Failure to meet the risk assessment policy and procedures requirements listed below could result in incomplete and ineffective risk assessment policy, which could lead eventually to the loss of critical mission/business assets or to the disruption of organization operations, functions and services:  (i) the organization categorizes information and the information system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; (ii) the organization documents the security categorization results (including supporting rationale) in the security plan for the information system; and (iii) the organization ensures that the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative. | High | [Test: RA-2.1 - Security Categorization]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication Policy and Procedures [NIST 800-53 w/ DHS 4300A IA-1] | [Test: IA-1.1 - Identification and Authentication Policy and Procedures]  Not Entered  [Test: IA-1.2 - Identification and Authentication Policy and Procedures]  Not Entered | Failure to meet the identification and authentication policy and procedures requirements listed below could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data:  (i) the organization defines the frequency of identification and authentication policy reviews/updates; (ii) the organization reviews/updates identification and authentication policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of identification and authentication procedure reviews/updates;  (iv) the organization reviews/updates identification and authentication procedures in accordance with organization-defined frequency.  Failure to meet the identification and authentication policy and procedures requirements listed below could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data:  (i) the organization develops and formally documents identification and authentication policy; (ii) the organization identification and authentication policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented identification and authentication policy to elements within the organization having associated identification and authentication roles and responsibilities; (iv) the organization develops and formally documents identification and authentication procedures; (v) the organization identification and authentication procedures facilitate implementation of the identification and authentication policy and associated identification and authentication controls; and (vi) the organization disseminates formal documented identification and authentication procedures to elements within the organization having associated identification and authentication roles and responsibilities. | High | [Test: IA-1.1 - Identification and Authentication Policy and Procedures]  Not Entered  [Test: IA-1.2 - Identification and Authentication Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Media Use [NIST 800-53 w/ DHS 4300A MP-7] | [Test: MP-7.1 - Media Use]  Not Entered | Failure to ensure that the organization restricts/prohibits the use of organization-defined types of information system media on organization-defined information systems or system components using organization-defined security safeguards could result in the disclosure of critical and sensitive mission/business information that may have been contained in the media. | High | [Test: MP-7.1 - Media Use]  Not Entered |  |
| [E-# OR W-#] | Process Isolation [NIST 800-53 w/ DHS 4300A SC-39] | [Test: SC-39.1 - Process Isolation]  Not Entered | Failure to ensure that the information system maintains a separate execution domain for each executing process could leave the system vulnerable to improper utilization of resources due to unmonitored activity of access. | High | [Test: SC-39.1 - Process Isolation]  Not Entered |  |
| [E-# OR W-#] | Sharing of Personal Passwords [NIST 800-53 w/ DHS 4300A AC-1 (DHS-5.1.1.c)] | [Test: AC-1(DHS-5.1.1.c) - Sharing of Personal Passwords]  Not Entered | Failure to prevent DHS users to share personal passwords could leave the information system vulnerable to unauthorized access, impersonation, and brute force attacks. | High | [Test: AC-1(DHS-5.1.1.c) - Sharing of Personal Passwords]  Not Entered |  |
| [E-# OR W-#] | Authority to Collect [NIST 800-53 w/ DHS 4300A PRIV-AP-1] | [Test: AP-1.1 - Authority to Collect]  Not Entered | Failure to meet the privacy control requirements for collecting PIIs listed below could lead to unauthorized disclosure of personal identifiable information:  (i) the organization identifies the legal bases that authorize a particular personally identifiable information (PII) collection or activity that impacts privacy; and, (ii) the organization specifies in their notices the purpose(s) for which PII is collected. | High | [Test: AP-1.1 - Authority to Collect]  Not Entered |  |
| [E-# OR W-#] | Risk Assessment Policy and Procedures [NIST 800-53 w/ DHS 4300A RA-1] | [Test: RA-1.1 - Risk Assessment Policy and Procedures]  Not Entered  [Test: RA-1.2 - Risk Assessment Policy and Procedures]  Not Entered | Failure to meet the risk assessment policy and procedures requirements listed below could lead eventually to the loss of critical mission/business assets or to the disruption of organization operations, functions and services:  (i) the organization develops and formally documents risk assessment policy; (ii) the organization risk assessment policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented risk assessment policy to elements within the organization having associated risk assessment roles and responsibilities; (iv) the organization develops and formally documents risk assessment procedures; (v) the organization risk assessment procedures facilitate implementation of the risk assessment policy and associated risk assessment controls; and (vi) the organization disseminates formal documented risk assessment procedures to elements within the organization having associated risk assessment roles and responsibilities.  Failure to meet the risk assessment policy and procedures requirements listed below could result in incomplete and ineffective risk assessment policy, which could lead eventually to the loss of critical mission/business assets or to the disruption of organization operations, functions and services:  (i) the organization defines the frequency of risk assessment policy reviews/updates; (ii) the organization reviews/updates risk assessment policy in accordance with organization-defined frequency; and (iii) the organization defines the frequency of risk assessment procedure reviews/updates; (iv) the organization reviews/updates risk assessment procedures in accordance with organization-defined frequency. | High | [Test: RA-1.1 - Risk Assessment Policy and Procedures]  Not Entered  [Test: RA-1.2 - Risk Assessment Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8] | [Test: CM-8.1 - Information System Component Inventory]  Not Entered | Failure to meet the information system component inventory requirements listed below could lead to the loss of critical resources due to the absence of tracking or due to the lack of the list of accountable personnel:  (i) the organization defines information deemed necessary to achieve effective property accountability; and (ii) the organization develops, documents, and maintains an inventory of information system components that:   * accurately reflects the current information system; * is consistent with the authorization boundary of the information system; * is at the level of granularity deemed necessary for tracking and reporting; * includes organization-defined information deemed necessary to achieve effective property accountability; and * is available for review and audit by designated organizational officials. | High | [Test: CM-8.1 - Information System Component Inventory]  Not Entered |  |
| [E-# OR W-#] | Security Authorization Process [NIST 800-53 w/ DHS 4300A PM-10] | [Test: PM-10.1 - Security Authorization Process]  Not Entered | Failure to meet the security authorization process requirements listed below could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization manages (i.e., documents, tracks, and reports) the security state of organizational information systems and the environments in which those systems operate through security authorization processes; (ii) the organization designates individuals to fulfill specific roles and responsibilities within the organizational risk management process; and (iii) the organization fully integrates the security authorization processes into an organization-wide risk management program. | High | [Test: PM-10.1 - Security Authorization Process]  Not Entered |  |
| [E-# OR W-#] | Architecture and Provisioning for Name/Address Resolution Service [NIST 800-53 w/ DHS 4300A SC-22] | [Test: SC-22.1 - Architecture and Provisioning for Name/Address Resolution Service]  Not Entered | Failure to ensure that the information systems that collectively provide name/address resolution service for an organization are fault-tolerant and implement internal/external role separation could result in the loss of system integrity and stability, which could lead to the disclosure of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SC-22.1 - Architecture and Provisioning for Name/Address Resolution Service]  Not Entered |  |
| [E-# OR W-#] | Personnel Termination [NIST 800-53 w/ DHS 4300A PS-4] | [Test: PS-4.1 - Personnel Termination]  Not Entered | Failure of the organization to determine the following requirements upon termination of individual employment could lead to expose the confidentiality, integrity and availability of data information and system:  (i) the organization disables information system access within organization-defined time period; (ii) the organization terminates/revokes any authenticators/credentials associated with the individual; (iii) the organization includes discussion of organization-defined information security topics in exit interviews; and, (iv) the organization retrieves all security-related organizational information system-related property. | High | [Test: PS-4.1 - Personnel Termination]  Not Entered |  |
| [E-# OR W-#] | Protection of Audit Information [NIST 800-53 w/ DHS 4300A AU-9] | [Test: AU-9.1 - Protection of Audit Information]  Not Entered | Failure of the information system to protect audit information and audit tools from unauthorized access, modification, and deletion could result in the loss of integrity of the audit information or of the audit tools, which could invalidate any result of forensic investigation. | High | [Test: AU-9.1 - Protection of Audit Information]  Not Entered |  |
| [E-# OR W-#] | Mission/Business Process Definition [NIST 800-53 w/ DHS 4300A PM-11] | [Test: PM-11.1 - Mission/Business Process Definition]  Not Entered | Failure to meet the mission/business process definition requirements listed below could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and (ii) the organization determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until an achievable set of protection needs is obtained. | High | [Test: PM-11.1 - Mission/Business Process Definition]  Not Entered |  |
| [E-# OR W-#] | Permitted Actions without Identification or Authentication [NIST 800-53 w/ DHS 4300A AC-14] | [Test: AC-14.1 - Permitted Actions without Identification or Authentication]  Not Entered | Failure of the organization to identify and document specific user actions that can be performed on the information system without identification or authentication could further encourage an attacker to try and break into the system using such user actions not requiring identification and authentication:  (i) the organization identifies specific user actions that can be performed on the information system without identification or authentication; and (ii) the organization documents and provides supporting rationale in the security plan for the information system, user actions not requiring identification and authentication. | High | [Test: AC-14.1 - Permitted Actions without Identification or Authentication]  Not Entered |  |
| [E-# OR W-#] | Personnel Screening [NIST 800-53 w/ DHS 4300A PS-3] | [Test: PS-3.1 - Personnel Screening]  Not Entered | Failure to meet the requirements for personnel screening indicated below could risk data being compromised by such individuals:  (i) the organization screens individuals prior to authorizing access to the information system; and (ii) the organization defines conditions requiring re-screening and, where re-screening is so indicated, the frequency of such re-screening. | High | [Test: PS-3.1 - Personnel Screening]  Not Entered |  |
| [E-# OR W-#] | Maintenance Personnel [NIST 800-53 w/ DHS 4300A MA-5] | [Test: MA-5.1 - Maintenance Personnel]  Not Entered | Failure to meet the requirements for maintenance personnel listed below could lead to the compromise the system or the misuse of data being processed, transported, or stored inside the system:  (i) the organization establishes a process for maintenance personnel authorization; (ii) the organization maintains a current list of authorized maintenance organizations or personnel; and (iii) personnel performing maintenance on the information system either have the required access authorizations or are supervised by designated organizational personnel with the required access authorizations and technical competence deemed necessary to supervise information system maintenance. | High | [Test: MA-5.1 - Maintenance Personnel]  Not Entered |  |
| [E-# OR W-#] | Information System Backup [NIST 800-53 w/ DHS 4300A CP-9] | [Test: CP-9.1 - Information System Backup]  Not Entered  [Test: CP-9.2 - Information System Backup]  Not Entered | Failure of the organization to protect backup information at the designated storage locations could lead to the disruption of critical mission/business functions, operations, and processes.  Failure to meet the information system backup requirements listed below could affect the media reliability and information integrity:  (i) the organization defines the frequency of conducting user-level information backups to support recovery time objectives and recovery point objectives; (ii) the organization defines the frequency of conducting system-level information backups to support recovery time objectives and recovery point objectives; (iii) the organization defines the frequency of conducting information system documentation backups (including security-related information) to support recovery time objectives and recovery point objectives;  (iv) the organization backs up user-level information in accordance with the organization-defined frequency; (v) the organization backs up system-level information in accordance with the organization-defined frequency; and (vi) the organization backs up information system documentation in accordance with the organization-defined frequency. | High | [Test: CP-9.1 - Information System Backup]  Not Entered  [Test: CP-9.2 - Information System Backup]  Not Entered |  |
| [E-# OR W-#] | Audit and Accountability Policy and Procedures [NIST 800-53 w/ DHS 4300A AU-1] | [Test: AU-1.1 - Audit and Accountability Policy and Procedures]  Not Entered  [Test: AU-1.2 - Audit and Accountability Policy and Procedures]  Not Entered | Failure to meet the requirements for audit and accountability policy and procedures listed below could result in inaccurate audit and accountability reports:   (i) the organization develops and formally documents audit and accountability policy; (ii) the organization audit and accountability policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented audit and accountability policy to elements within the organization having associated audit and accountability roles and responsibilities; (iv) the organization develops and formally documents audit and accountability procedures; (v) the organization audit and accountability procedures facilitate implementation of the audit and accountability policy and associated audit and accountability controls; and (vi) the organization disseminates formal documented audit and accountability procedures to elements within the organization having associated audit and accountability roles and responsibilities.  Failure to meet the requirements of the audit and accountability policy meets the requirements indicated below could result in unsuitable or erroneous audit reports:  (i) the organization defines the frequency of audit and accountability policy reviews/updates; (ii) the organization reviews/updates audit and accountability policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of audit and accountability procedure reviews/updates; and (iv) the organization reviews/updates audit and accountability procedures in accordance with organization-defined frequency. | High | [Test: AU-1.1 - Audit and Accountability Policy and Procedures]  Not Entered  [Test: AU-1.2 - Audit and Accountability Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8] | [Test: IA-8.1 - Identification and Authentication(Non-Organizational Users)]  Not Entered | Failure to ensure that the information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users) could leave the system vulnerable to unauthorized access and intrusion. | High | [Test: IA-8.1 - Identification and Authentication(Non-Organizational Users)]  Not Entered |  |
| [E-# OR W-#] | Audit Storage Capacity [NIST 800-53 w/ DHS 4300A AU-4] | [Test: AU-4.1 - Audit Storage Capacity]  Not Entered | Failure to meet the audit storage capacity requirements indicated below could result in lost data, which could prove detrimental to the success of a forensic or audit report:  (i) the organization allocates audit record storage capacity; and, (ii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded. | High | [Test: AU-4.1 - Audit Storage Capacity]  Not Entered |  |
| [E-# OR W-#] | Privacy Notice [NIST 800-53 w/ DHS 4300A PRIV-TR-1] | [Test: TR-1.1 - Privacy Notice]  Not Entered | Failure to meet the privacy notice requirements listed below increases the risk to unauthorized disclosure of personally identifiable information:  (i) the organization provides effective notice to the public and to individuals regarding:   * its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); * authority for collecting PII; * the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and * the ability to access and have PII amended or corrected if necessary;   (ii) the organization describes:   * the PII the organization collects and the purpose(s) for which it collects that information; * how the organization uses PII internally; * whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; * whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; * how individuals may obtain access to PII; and * how the PII will be protected; and   (iii) the organization revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change. | High | [Test: TR-1.1 - Privacy Notice]  Not Entered |  |
| [E-# OR W-#] | Incident Handling [NIST 800-53 w/ DHS 4300A IR-4] | [Test: IR-4.1 - Incident Handling]  Not Entered | Failure to meet the requirements for incident handling listed below could lead to the compromise of the system or of the data in the system:  (i) the organization implements an incident handling capability for security incidents that includes:   * preparation; * detection and analysis; * containment; * eradication; and * recovery;   (ii) the organization coordinates incident handling activities with contingency planning activities; and (iii) the organization incorporates lessons learned from ongoing incident handling activities into:   * incident response procedures; * training; and * testing/exercises; and   (iv) the organization implements the resulting changes to incident response procedures, training and testing/exercise accordingly. | High | [Test: IR-4.1 - Incident Handling]  Not Entered |  |
| [E-# OR W-#] | Allocation of Resources [NIST 800-53 w/ DHS 4300A SA-2] | [Test: SA-2.1 - Allocation of Resources]  Not Entered | Failure to meet the resource allocation requirement listed below could result in the organization lacking the required security control being acquired and implemented, which could cause the loss of critical mission/business assets or the disruption of organization operations, functions and services:  (i) the organization includes a determination of the information security requirements for the information system in mission/business process planning; (ii) the organization determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and, (iii) the organization establishes a discrete line item for information security in organizational programming and budgeting documentation. | High | [Test: SA-2.1 - Allocation of Resources]  Not Entered |  |
| [E-# OR W-#] | Accounting of Disclosures [NIST 800-53 w/ DHS 4300A PRIV-AR-8] | [Test: AR-8.1 - Accounting of Disclosures]  Not Entered | Failure to meet the accounting of disclosure requirements listed below could eventually lead to the loss of critical resources due to the absence of tracking process that could detect missing critical privacy information in a timely fashion:  (i) the organization keeps an accurate accounting of disclosures of information held in each system of records under its control, including:   * date, nature, and purpose of each disclosure of a record; and * name and address of the person or agency to which the disclosure was made;   (ii) the organization retains the accounting of disclosures for the life of the record or five years after the disclosure is made, whichever is longer; and, (iii) the organization makes the accounting of disclosures available to the person named in the record upon request. | High | [Test: AR-8.1 - Accounting of Disclosures]  Not Entered |  |
| [E-# OR W-#] | Insider Threat Program [NIST 800-53 w/ DHS 4300A PM-12] | [Test: PM-12.1 - Insider Threat Program]  Not Entered | Failure to ensure that the organization implements an insider threat program that includes a cross-discipline insider threat incident handling team could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: PM-12.1 - Insider Threat Program]  Not Entered |  |
| [E-# OR W-#] | Consent [NIST 800-53 w/ DHS 4300A PRIV-IP-1] | [Test: IP-1.1 - Consent]  Not Entered | Failure to meet the consent requirements for individual participation and redress listed below increases the risk to unauthorized disclosure of personally identifiable information:  (i) the organization provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; (ii) the organization provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; (iii) the organization obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and (iv) the organization ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII. | High | [Test: IP-1.1 - Consent]  Not Entered |  |
| [E-# OR W-#] | Enterprise Architecture [NIST 800-53 w/ DHS 4300A PM-7] | [Test: PM-7.1 - Enterprise Architecture]  Not Entered | Failure to ensure that the organization develops an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation could risk the exposure of essential information compromising the confidentiality, integrity and availability of the system. | High | [Test: PM-7.1 - Enterprise Architecture]  Not Entered |  |
| [E-# OR W-#] | External Information System Services [NIST 800-53 w/ DHS 4300A SA-9] | [Test: SA-9.1 - External Information System Services]  Not Entered | Failure to meet the external information system services requirements listed below could eventually lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services:  (i) the organization requires that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; (ii) the organization defines and documents government oversight and user roles and responsibilities with regard to external information system services; and, (iii) the organization employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. | High | [Test: SA-9.1 - External Information System Services]  Not Entered |  |
| [E-# OR W-#] | Physical Access Control [NIST 800-53 w/ DHS 4300A PE-3] | [Test: PE-3.1 - Physical Access Control]  Not Entered  [Test: PE-3.2 - Physical Access Control]  Not Entered | Failure to meet the requirements for physical access control listed below could lead to the compromise of the system or of the data in the system:  (i) the organization defines the frequency for conducting inventories of physical access devices; (ii) the organization inventories physical access devices in accordance with the organization-defined frequency; (iii) the organization defines the frequency of changes to combinations and keys; and (iv) the organization changes combinations and keys in accordance with the organization-defined frequency, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.  Failure to meet the requirements for physical access control listed below could lead to the compromise of the system or of the data in the system:  (i) the organization enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible); (ii) the organization verifies individual access authorizations before granting access to the facility; (iii) the organization controls entry to the facility containing the information system using physical access devices (e.g., keys, locks, combinations, card readers) and/or guards; (iv) the organization controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk; and (v) the organization secures keys, combinations, and other physical access devices. | High | [Test: PE-3.1 - Physical Access Control]  Not Entered  [Test: PE-3.2 - Physical Access Control]  Not Entered |  |
| [E-# OR W-#] | Internal Use [NIST 800-53 w/ DHS 4300A PRIV-UL-1] | [Test: UL-1.1 - Internal Use]  Not Entered | Failure to ensure that organization uses PII internally only for authorized purpose(s) increases the risk to loss, unauthorized access, or disclosure of privacy information. | High | [Test: UL-1.1 - Internal Use]  Not Entered |  |
| [E-# OR W-#] | Continuous Monitoring [NIST 800-53 w/ DHS 4300A CA-7] | [Test: CA-7.1 - Continuous Monitoring]  Not Entered | Failure to meet the continuous monitoring requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization establishes a continuous monitoring strategy and program; (ii) the organization defines the frequency for reporting the security state of the information system to appropriate organizational officials; (iii) the organization defines organizational officials to whom the security state of the information system should be reported; and (iv) the organization implements a continuous monitoring program that includes:   * a configuration management process for the information system and its constituent components; * a determination of the security impact of changes to the information system and environment of operation; * ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and * reporting the security state of the information system to appropriate organizational officials in accordance with organization-defined frequency. | High | [Test: CA-7.1 - Continuous Monitoring]  Not Entered |  |
| [E-# OR W-#] | Security Impact Analysis [NIST 800-53 w/ DHS 4300A CM-4] | [Test: CM-4.1 - Security Impact Analysis]  Not Entered | Failure to ensure that the organization analyzes changes to the information system to determine potential security impacts prior to change implementation could lead to the compromise of the system or of the data in the system. | High | [Test: CM-4.1 - Security Impact Analysis]  Not Entered |  |
| [E-# OR W-#] | Privacy-Enhanced System Design and Development [NIST 800-53 w/ DHS 4300A PRIV-AR-7] | [Test: AR-7.1 - Privacy-Enhanced System Design and Development]  Not Entered | Failure to ensure that the organization designs information systems to support privacy by automating privacy controls could promote a non-standard way of handling privacy control management functions resulting in inaccurate information critical to the operation of the system. | High | [Test: AR-7.1 - Privacy-Enhanced System Design and Development]  Not Entered |  |
| [E-# OR W-#] | Privacy Requirements for Contractors and Service Providers [NIST 800-53 w/ DHS 4300A PRIV-AR-3] | [Test: AR-3.1 - Privacy Requirements for Contractors and Service Providers]  Not Entered | Failure to meet the privacy requirements for contractors and service providers listed below could lead to personally identifiable information and other sensitive data to be modified and used by unauthorized users:  (i) the organization establishes privacy roles, responsibilities, and access requirements for contractors and service providers; and, (ii) the organization includes privacy requirements in contracts and other acquisition-related documents. | High | [Test: AR-3.1 - Privacy Requirements for Contractors and Service Providers]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6] | [Test: AU-6.1 - Audit Review, Analysis, and Reporting]  Not Entered  [Test: AU-6.2 - Audit Review, Analysis, and Reporting]  Not Entered | Failure of the organization to increase the level of audit monitoring and analysis activity whenever there is increased risk to organizational operations and assets, or to individuals, based on information from law enforcement organizations, the intelligence community, or other credible sources could result in the inability of the organization to track any security incident, which could lead to other severe security threats.  Failure to meet the audit review requirements listed below could result in the inability of the organization to track any security incident, which could lead to other severe security threats:  (i) the organization defines the frequency of information system audit record reviews and analyses; (ii) the organization reviews and analyzes information system audit records for indications of inappropriate or unusual activity in accordance with the organization-defined frequency; and, (iii) the organization reports findings of inappropriate/unusual activities, to designated organizational officials. | High | [Test: AU-6.1 - Audit Review, Analysis, and Reporting]  Not Entered  [Test: AU-6.2 - Audit Review, Analysis, and Reporting]  Not Entered |  |
| [E-# OR W-#] | Media Sanitization [NIST 800-53 w/ DHS 4300A MP-6] | [Test: MP-6.1 - Media Sanitization]  Not Entered | Failure to meet the media sanitization requirements indicated below could result in the disclosure of critical and sensitive mission/business information that may have been contained in the media:  (i) the organization sanitizes organization-defined information system media prior to disposal, release out of organizational control, or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and  (ii) the organization employs sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information. | High | [Test: MP-6.1 - Media Sanitization]  Not Entered |  |
| [E-# OR W-#] | Response to Audit Processing Failures [NIST 800-53 w/ DHS 4300A AU-5] | [Test: AU-5.1 - Response to Audit Processing Failures]  Not Entered | Failure to observe the requirements listed below for response to audit processing failures could result in the failure of disaster avoidance where data critical to an accurate audit report could be damaged without personnel responsible for its maintenance being alerted:  (i) the organization defines designated organizational officials to be alerted in the event of an audit processing failure; (ii) the information system alerts designated organizational officials in the event of an audit processing failure; (iii) the organization defines additional actions to be taken in the event of an audit processing failure; and, (iv) the information system takes the additional organization-defined actions in the event of an audit processing failure. | High | [Test: AU-5.1 - Response to Audit Processing Failures]  Not Entered |  |
| [E-# OR W-#] | Personnel Transfer [NIST 800-53 w/ DHS 4300A PS-5] | [Test: PS-5.1 - Personnel Transfer]  Not Entered | Failure to meet the requirements for personnel transfer listed below could risk disclosure of organizational information:  (i) the organization reviews logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the organization; (ii) the organization initiates organization-defined transfer or reassignment actions within organization-defined time period following the formal transfer action; (iii) the organization confirms ongoing operational need for current access authorizations; and (iv) the organization modifies access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. | High | [Test: PS-5.1 - Personnel Transfer]  Not Entered |  |
| [E-# OR W-#] | Temperature and Humidity Controls [NIST 800-53 w/ DHS 4300A PE-14] | [Test: PE-14.1 - Temperature and Humidity Controls]  Not Entered | Failure to meet the temperature and humidity controls requirements listed below could risk potential damage to the system and data/information due to high humidity or temperature level:  (i) the organization maintains temperature and humidity levels within the facility where the information system resides at organization-defined acceptable levels; and, (ii) the organization monitors temperature and humidity levels organization-defined frequency. | High | [Test: PE-14.1 - Temperature and Humidity Controls]  Not Entered |  |
| [E-# OR W-#] | System and Information Integrity Policy and Procedures [NIST 800-53 w/ DHS 4300A SI-1] | [Test: SI-1.1 - System and Information Integrity Policy and Procedures]  Not Entered  [Test: SI-1.2 - System and Information Integrity Policy and Procedures]  Not Entered | Failure to meet the system and information integrity policy and procedures requirements listed below results in the ineffective and incomplete system and information integrity policy, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization defines the frequency of system and information integrity policy reviews/updates; (ii) the organization reviews/updates system and information integrity policy in accordance with organization-defined frequency; (iii) the organization defines the frequency of system and information integrity procedure reviews/updates; and (iv) the organization reviews/updates system and information integrity procedures in accordance with organization-defined frequency.  Failure to meet the system and information integrity policy and procedures requirements listed below results in the ineffective system and information integrity policy, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes:  (i) the organization develops and formally documents system and information integrity policy; (ii) the organization system and information integrity policy addresses:   * purpose; * scope; * roles and responsibilities; * management commitment; * coordination among organizational entities; and * compliance;   (iii) the organization disseminates formal documented system and information integrity policy to elements within the organization having associated system and information integrity roles and responsibilities; (iv) the organization develops and formally documents system and information integrity procedures; (v) the organization system and information integrity procedures facilitate implementation of the system and information integrity policy and associated system and information integrity controls; and (vi) the organization disseminates formal documented system and information integrity procedures to elements within the organization having associated system and information integrity roles and responsibilities. | High | [Test: SI-1.1 - System and Information Integrity Policy and Procedures]  Not Entered  [Test: SI-1.2 - System and Information Integrity Policy and Procedures]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-4.5.2.a)] | [Test: SC-1(DHS-4.5.2.a) - Technical Controls for FAX machines]  Not Entered | Failure of the components to implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information could result in unsafe and ineffective communication systems, which could eventually lead to the loss of critical mission/business assets and information or to the disruption of DHS operations, functions and services. | High | [Test: SC-1(DHS-4.5.2.a) - Technical Controls for FAX machines]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-5.4.5.e)] | [Test: CM-6(DHS-5.4.5.e) - Use of File Transfer Protocol(FTP) Services]  Not Entered | Failure to meet the requirements for configuration settings listed below could lead to the compromise of the system or of the data in the system:  (i) the organization does not authorize File Transfer Protocol (FTP) connections to any DHS computer;  (ii) the organization uses secure connection protocols duly approved by the Component; and  (iii) the secure connection protocols used employ any of the following authentication methods:   * two factor * encryption * key exchange | High | [Test: CM-6(DHS-5.4.5.e) - Use of File Transfer Protocol(FTP) Services]  Not Entered |  |
| [E-# OR W-#] | Media Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A MP-1 (DHS-3.14.5.b)] | [Test: MP-1(DHS-3.14.5.b) - Removal of PII]  Not Entered | Failure to meet the media protection policy and procedures requirements indicated below could result in an ineffective media protection, which could eventually lead to the organization losing critical mission/business assets in the form of unauthorized or unintentional disclosure of information:  (i) PII and sensitive can be physically removed from an information system;  (ii) the Security Plan documents the specific procedures, training, and accountability measures in place when PII and sensitive PII are removed from the IS. | High | [Test: MP-1(DHS-3.14.5.b) - Removal of PII]  Not Entered |  |
| [E-# OR W-#] | Security Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A PL-1 (DHS-3.14.7.d)] | [Test: PL-1(DHS-3.14.7.d) - E-Authentication]  Not Entered | Failure of the components to ensure that each Security Plan reflects the e-authentication status of the respective systems could result in the weak security stance of the organization due to ineffective and incomplete security planning policy and procedures. | High | [Test: PL-1(DHS-3.14.7.d) - E-Authentication]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13 (DHS-5.5.1.a)] | [Test: SC-13(DHS-5.5.1.a) - Encryption Standards]  Not Entered | Failure to determine if systems requiring encryption complied the following methods which listed below methods could lead to the organization to face litigations because of offenses related to non-compliance of these premises:  (i) Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2 (Note: The use of triple DES [3DES] and FIPS 140-1 is no longer permitted.). (ii) NSA Type 2 or Type 1 encryption. | High | [Test: SC-13(DHS-5.5.1.a) - Encryption Standards]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication Policy and Procedures [NIST 800-53 w/ DHS 4300A IA-1 (DHS-3.14.7.f)] | [Test: IA-1(DHS-3.14.7.f) - PIV Credentials]  Not Entered | Failure to upgrade the existing physical and logical access control systems to use PIV credentials could weaken the overall security posture of the system due to lack of compliance to known standards and policies. | High | [Test: IA-1(DHS-3.14.7.f) - PIV Credentials]  Not Entered |  |
| [E-# OR W-#] | Security Categorization [NIST 800-53 w/ DHS 4300A RA-2 (DHS-3.14.2.e)] | [Test: RA-2(DHS-3.14.2.e) - Confidentiality for Privacy Systems]  Not Entered | Failure to ensure that the confidentiality security object for Privacy Sensitive Systems are assigned an impact level of moderate or higher could result in ineffective controls and increased information security risks. | High | [Test: RA-2(DHS-3.14.2.e) - Confidentiality for Privacy Systems]  Not Entered |  |
| [E-# OR W-#] | Security Assessment and Authorization Policies and Procedures [NIST 800-53 w/ DHS 4300A CA-1 (DHS-3.9.m)] | [Test: CA-1(DHS-3.9.m) - Use of IACS for Security Authorization]  Not Entered | Failure to ensure that all DHS systems are authorized using the approved automated IACS tools by the DHS CISO could result in a weak security stance of the organization due to security threats that may not have been addressed accordingly or completely by organizational personnel with certification, accreditation and assessment roles and responsibilities. | High | [Test: CA-1(DHS-3.9.m) - Use of IACS for Security Authorization]  Not Entered |  |
| [E-# OR W-#] | Non-Local Maintenance [NIST 800-53 w/ DHS 4300A MA-4 (DHS-5.4.4.c)] | [Test: MA-4(DHS-5.4.4.c) - Remote Maintenance Paths]  Not Entered | Failure to ensure that the components encrypt the remote maintenance paths to the firewalls and PEPs could leave stored or transmitted information susceptible to unauthorized access, or could lead to incompatible implementations that hinder or prevent normal user operations. | High | [Test: MA-4(DHS-5.4.4.c) - Remote Maintenance Paths]  Not Entered |  |
| [E-# OR W-#] | Life Cycle Support [NIST 800-53 w/ DHS 4300A SA-3] | [Test: SA-3.1 - System Development Life Cycle]  Not Entered | Failure to meet the requirements for life cycle support listed below could result to a less-secured system that could open the organization to exploits by any attacker:  (i) the organization manages the information system using organization-defined system development life cycle] that incorporates information security considerations;  (ii) the organization defines and documents information security roles and responsibilities throughout the system development life cycle;  (iii) the organization identifies individuals having information security roles and responsibilities; and  (iv) the organization integrates the organizational information security risk management process into system development life cycle activities. | High | [Test: SA-3.1 - System Development Life Cycle]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4] | [Test: SA-4.1 - Acquisition Process]  Not Entered | Failure to ensure that the organization includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, guidelines, and organizational mission/business needs could try to exploit using various vectors and compromise the system or the data in the system:  (i) Security functional requirements; (ii) Security strength requirements; (iii) Security assurance requirements; (iv) Security-related documentation requirements; (v) Requirements for protecting security-related documentation; (vi) Description of the information system development environment and environment in which the system is intended to operate; and (vii) Acceptance criteria. | High | [Test: SA-4.1 - Acquisition Process]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.d)] | [Test: CA-3(DHS-5.4.3.d) - ISA Reissuance]  Not Entered | Failure to reissue ISAs every three years or whenever changes are made to interconnected systems could lead to compromise of the system or of the data in the system. | High | [Test: CA-3(DHS-5.4.3.d) - ISA Reissuance]  Not Entered |  |
| [E-# OR W-#] | Denial-of-Service Protection [NIST 800-53 w/ DHS 4300A SC-5] | [Test: SC-5.1 - Denial of Service Protection]  Not Entered | Failure to ensure that the information system protects against or limits the effects of the following types of denial of service attacks organization-defined types of denial of service attacks or reference to source for such information by employing organization-defined security safeguards could result in a system that lacks stability and integrity causing the unavailability of the system or the data in the system to authorized users. | High | [Test: SC-5.1 - Denial of Service Protection]  Not Entered |  |
| [E-# OR W-#] | Security Training [NIST 800-53 w/ DHS 4300A AT-3] | [Test: AT-3.1 - Role-Based Security Training]  Not Entered | Failure to meet the security training requirements indicated below could enable would-be attackers to take advantage of unidentified accounts with significant information system security privileges and cause damage to the information system:  (i) the organization provides role-based security-related training before authorizing access to the system or performing assigned duties, and when required by system changes; (ii) the organization defines the frequency of refresher role-based security-related training; and, (iii) the organization provides refresher role-based security-related training in accordance with the organization-defined frequency. | High | [Test: AT-3.1 - Role-Based Security Training]  Not Entered |  |
| [E-# OR W-#] | Collaborative Computing Devices [NIST 800-53 w/ DHS 4300A SC-15 (DHS-4.5.3.a)] | [Test: SC-15(DHS-4.5.3.a) - Video Teleconference Protections]  Not Entered | Failure of the components to implement controls to ensure that only authorized individuals are able to participate in each videoconference could allow the disclosure of critical DHS information. | High | [Test: SC-15(DHS-4.5.3.a) - Video Teleconference Protections]  Not Entered |  |
| [E-# OR W-#] | Malicious Code Protection [NIST 800-53 w/ DHS 4300A SI-3 (DHS-5.4.6.g)] | [Test: SI-3(DHS-5.4.6.g) - Email Monitoring for Malware]  Not Entered | Failure to ensure that DHS email gateway Steward provides email monitoring for malware activity at the gateway could result in difficulty in audit and in investigation if an intrusion occurs. | High | [Test: SI-3(DHS-5.4.6.g) - Email Monitoring for Malware]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13 (DHS-5.7.d)] | [Test: SC-13(DHS-5.7.d) - Cryptography Requirements]  Not Entered | Failure to ensure that components use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography could lead to the DHS to face litigations because of offenses related to non-compliance of these premises. | High | [Test: SC-13(DHS-5.7.d) - Cryptography Requirements]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication Policy and Procedures [NIST 800-53 w/ DHS 4300A IA-1 (DHS-3.14.7.a)] | [Test: IA-1(DHS-3.14.7.a) - Online Transactions]  Not Entered | Failure to apply e-authentication requirements for systems that allow online transactions could allow the system to become vulnerable to external attacks or unauthorized access. Data availability and/or integrity can be affected. | High | [Test: IA-1(DHS-3.14.7.a) - Online Transactions]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8 (2)] | [Test: IA-8(2).1 - Acceptance Of Third-Party Credentials]  Not Entered | Failure to ensure that the organization uses only FICAM-approved third-party credentials could weaken its security posture, resulting to the ineffectiveness of the identification and authentication policy. | High | [Test: IA-8(2).1 - Acceptance Of Third-Party Credentials]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (DHS-5.7.b)] | [Test: SA-4(DHS-5.7.b) - COTS Evaluation]  Not Entered | Failure to ensure that the strong preference are given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) The NIST FIPS validation program. (ii) The National Security Agency (NSA)/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program. (iii) The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement. | High | [Test: SA-4(DHS-5.7.b) - COTS Evaluation]  Not Entered |  |
| [E-# OR W-#] | Security Assessment and Authorization Policies and Procedures [NIST 800-53 w/ DHS 4300A CA-1 (DHS-3.18.c)] | [Test: CA-1(DHS-3.18.c) - Cloud Environment Usage]  Not Entered | Failure to meet the cloud usage environment requirements listed below could result in a weak security stance of the organization due to security threats that may not have been addressed accordingly or completely by organizational personnel with certification, accreditation and assessment roles and responsibilities:  (i) the organization employs the use of cloud environments; (ii) the organization follow standard cloud usage environment procedures , which include:   * a completed security authorization package; and, * an ATO signed by the component or DHS-designated risk executive. | High | [Test: CA-1(DHS-3.18.c) - Cloud Environment Usage]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (DHS-5.3.b)] | [Test: AU-6(DHS-5.3.b) - Audit Records for Financial Systems and PII]  Not Entered | Failure to conduct monthly audit reviews for financial systems or PII-hosted systems could allow unauthorized access to go unnoticed increasing the risk that unauthorized persons could gain access to sensitive information. | High | [Test: AU-6(DHS-5.3.b) - Audit Records for Financial Systems and PII]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-5.4.5.d)] | [Test: CM-6(DHS-5.4.5.d) - Use of Telnet]  Not Entered | Failure to meet the requirements for configuration settings listed below could lead to the compromise of the system or of the data in the system:  (i) the organization does not authorize Telnet connections to any DHS computer;  (ii) the organization uses Secure Shell (SSH) connection protocols duly approved by the Component; and  (iii) the SSH employ any of the following secure authentication methods:   * two factor * encrypted * key exchange | High | [Test: CM-6(DHS-5.4.5.d) - Use of Telnet]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (DHS-5.4.1.b)] | [Test: AC-17(DHS-5.4.1.b) - Remote Access Connection Management]  Not Entered | Failure to meet the required remote access control policy and procedures listed below could result in a weaker security posture as a consequence of a failed audit process, the non-accountability of critical actions, and ignorance to the policy being implemented for the organization:  (i) the Components centrally manage all remote access and dial-in connections to their systems;  (ii) the Components ensure that remote access and approved dial-in capabilities provide the following access control mechanisms for sensitive information throughout transmission:   * strong authentication * two-factor authentication * audit capabilities * protection   (ii) two-factor authentication is only allowed during remote access if one of the factors is provided by a device separate from the computer gaining access;  (iv) any two-factor authentication is based on Department-controlled certificates or hardware tokens issued directly to each authorized user; and  (v) remote access solutions comply with the encryption requirements of FIPS 140-2, Security Requirements for Cryptographic Modules. | High | [Test: AC-17(DHS-5.4.1.b) - Remote Access Connection Management]  Not Entered |  |
| [E-# OR W-#] | Secure Name/Address Resolution Service (Recursive or Caching Resolver) [NIST 800-53 w/ DHS 4300A SC-21] | [Test: SC-21.1 - Secure Name / Address Resolution Service(Recursive or Caching Resolver)]  Not Entered | Failure of the information system, that provides name/address resolution service for local clients, to perform data origin authentication and data integrity verification on the resolution responses it receives from authoritative sources when requested by client systems could lead to the complete compromise of the system. | High | [Test: SC-21.1 - Secure Name / Address Resolution Service(Recursive or Caching Resolver)]  Not Entered |  |
| [E-# OR W-#] | Information Output Handling and Retention [NIST 800-53 w/ DHS 4300A SI-12] | [Test: SI-12.1 - Information Handling and Retention]  Not Entered | Failure to ensure that the organization handles and retains information within the information system and information output from the system in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements could result in the disclosure of critical/sensitive information or data, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-12.1 - Information Handling and Retention]  Not Entered |  |
| [E-# OR W-#] | System Use Notification [NIST 800-53 w/ DHS 4300A AC-8 (DHS-4.8.5.d)] | [Test: AC-8(DHS-4.8.5.d) - Governement Funded Office Equipment]  Not Entered | Failure to audit and/or monitor all government office equipment and DHS systems/computers using the criteria below could allow unauthorized activities (including insider threat) and other form of intrusions to go undetected.  Monitoring criteria: (a) Tracking of internal and external transactions (e.g. Internet access). (b) Auditing of stored data on local, network storage devices, and removable media. | High | [Test: AC-8(DHS-4.8.5.d) - Governement Funded Office Equipment]  Not Entered |  |
| [E-# OR W-#] | Contingency Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A CP-1 (DHS-3.5.1.a)] | [Test: CP-1(DHS-3.5.1.a) - Continuity of Operations Planning]  Not Entered | Failure to develop and employ continuity of operations (CO) planning policies could leave the organization unprepared for any incident when it occurs, which could lead to the compromise of the system or of the data in the system. | High | [Test: CP-1(DHS-3.5.1.a) - Continuity of Operations Planning]  Not Entered |  |
| [E-# OR W-#] | Physical and Environmental Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A PE-1 (DHS-4.6.2.3.b)] | [Test: PE-1(DHS-4.6.2.3.b) - Video, IR, and RF Signals]  Not Entered | Failure to ensure that the functions that transmit or receive video, infrared (IR), or radio frequency (RF) signals are disabled in areas where sensitive information is discussed could result in the inadvertent transmission of sensitive information to unauthorized individuals. | High | [Test: PE-1(DHS-4.6.2.3.b) - Video, IR, and RF Signals]  Not Entered |  |
| [E-# OR W-#] | Life Cycle Support [NIST 800-53 w/ DHS 4300A SA-3 (DHS-3.6.c)] | [Test: SA-3(DHS-3.6.c) - Custom Code]  Not Entered | Failure to meet the requirements for life cycle support listed below could result to a less-secured system that could open the organization to exploits by any attacker:  (i) the Program Manager review, approve, and sign all custom-developed code prior to deployment into production environments; (ii) the Program Manager may delegate this authority to another DHS employee in writing and the authority is not delegated to contractor personnel. | High | [Test: SA-3(DHS-3.6.c) - Custom Code]  Not Entered |  |
| [E-# OR W-#] | Security Authorization [NIST 800-53 w/ DHS 4300A CA-6 (DHS-3.9.h)] | [Test: CA-6(DHS-3.9.h) - DHS Security Authorization]  Not Entered | Failure to meet the security authorization requirements listed below could lead to compromise of the system or of the data in the system:  (i) the components authorize systems at Initial Operating Capability, every three (3) years after, or whenever major changes occurs; and  (ii) an Authority to Operate (ATO) of six (6) months or less receives an ATO authorization period waiver from the DHS CISO before submission to the AO for the final decision. | High | [Test: CA-6(DHS-3.9.h) - DHS Security Authorization]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-3.7.e)] | [Test: CM-6(DHS-3.7.e) - USGCB Requirements]  Not Entered | Failure to meet the workstation's baseline configuration requirements listed below could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or of systems that need configuration updates:  (i) the organization maintains a baseline configuration for workstations in accordance with DHS guidance on the U.S. Government Configuration Baseline (USGCB); and  (ii) the baseline configuration for workstations include installation of DHS Common Policy Object Identifier (OID), Common Policy Framework Root CA Certificate, and the DHS Principal CA Certificate. | High | [Test: CM-6(DHS-3.7.e) - USGCB Requirements]  Not Entered |  |
| [E-# OR W-#] | Collaborative Computing Devices [NIST 800-53 w/ DHS 4300A SC-15 (DHS-4.5.3.b)] | [Test: SC-15(DHS-4.5.3.b) - Video Teleconference Protections]  Not Entered | Failure of the components to ensure that the appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference could lead to disclosure of information that could be used by an attacker for further attacks. | High | [Test: SC-15(DHS-4.5.3.b) - Video Teleconference Protections]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (DHS-4.8.2.a)] | [Test: PL-4(DHS-4.8.2.a) - Laptop Encryption]  Not Entered | Failure to meet the rules of behavior requirements listed below could leave the users unaware of the required behavior with regard to information usage, which could lead to the user inadvertently abusing the information system resources:  (i) explicit restrictions on the use of social networking sites; (ii) posting information on commercial Web sites; and (iii) sharing information system account information. | High | [Test: PL-4(DHS-4.8.2.a) - Laptop Encryption]  Not Entered |  |
| [E-# OR W-#] | Security Awareness [NIST 800-53 w/ DHS 4300A AT-2] | [Test: AT-2.1 - Security Awareness Training]  Not Entered | Failure to meet the security awareness requirements indicated below could result in the organization's personnel's incomplete knowledge of the organization's security policy:  (i) the organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes; (ii) the organization defines the frequency of refresher security awareness training; and, (iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency. | High | [Test: AT-2.1 - Security Awareness Training]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-4.5.3.b)] | [Test: SC-1(DHS-4.5.3.b) - Transmission Controls]  Not Entered | Failure of the components to ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference could result in unsafe and ineffective communication systems, which could eventually lead to the loss of critical mission/business assets and information or to the disruption of DHS operations, functions and services. | High | [Test: SC-1(DHS-4.5.3.b) - Transmission Controls]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (DHS-5.4.6.f)] | [Test: AU-6(DHS-5.4.6.f) - Mail Server Administration]  Not Entered | Failure to employ mail server administration procedures could result in the loss of the integrity of the system due to untimely detection of threats or attacks. | High | [Test: AU-6(DHS-5.4.6.f) - Mail Server Administration]  Not Entered |  |
| [E-# OR W-#] | Secure Name/Address Resolution Service (Authoritative Source) [NIST 800-53 w/ DHS 4300A SC-20 (DHS-5.4.3.k)] | [Test: SC-20(DHS-5.4.3.k) - DHS Secure Name / Address Resolution Service]  Not Entered | Failure to ensure that all DHS systems connected to OneNet and operating at moderate or high level are utilized secure Name/Address resolution service provided by DHS OneNet could risk the integrity and stability of the system. | High | [Test: SC-20(DHS-5.4.3.k) - DHS Secure Name / Address Resolution Service]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-5.5.3.j)] | [Test: SC-1(DHS-5.5.3.j) - DHS FPKI]  Not Entered | Failure to meet the DHS FPKI requirements listed below could lead to non-compliance with the organization's policies, procedures, privacy requirements, agreements or contracts:  (i) the organization ensures that every human subscriber has read, understand, and signed a “DHS PKI Human Subscriber Acknowledgement of Responsibilities” as a pre-condition for receiving certificates from a DHS CA; and (ii) the organization ensures that all signed PKI Human Subscriber Agreements are maintained by the DHS PKI Registrar. | High | [Test: SC-1(DHS-5.5.3.j) - DHS FPKI]  Not Entered |  |
| [E-# OR W-#] | System and Services Acquisition Policy and Procedures [NIST 800-53 w/ DHS 4300A SA-1 (DHS-3.1.g)] | [Test: SA-1(DHS-3.1.g) - DHS Enterprise Architecture and Security Architecture]  Not Entered | Failure of the component CISOs /ISSMs to ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference model (TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/CISO could result in the acquisition of a system/service that would expose the organization to various threats and exploits, which could cause the loss of critical mission/business assets or the disruption of organization operations, functions and services. | High | [Test: SA-1(DHS-3.1.g) - DHS Enterprise Architecture and Security Architecture]  Not Entered |  |
| [E-# OR W-#] | Secure Name/Address Resolution Service (Authoritative Source) [NIST 800-53 w/ DHS 4300A SC-20] | [Test: SC-20.1 - Secure Name / Address Resolution Service(Authoritative Source)]  Not Entered | Failure to meet the requirements for secure name / address resolution service(authoritative source) listed below could lead to the disclosure of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes.  (i) the organization provides additional data origin and integrity artifacts along with the authoritative name resolution data the system returns in response to external name/address resolution queries; and (ii) the organization provides the means to indicate the security status of child zones and (if the child supports secure resolution services) to enable verification of a chain of trust among parent and child domains, when operating as part of a distributed, hierarchical namespace. | High | [Test: SC-20.1 - Secure Name / Address Resolution Service(Authoritative Source)]  Not Entered |  |
| [E-# OR W-#] | Audit Record Retention [NIST 800-53 w/ DHS 4300A AU-11 (DHS-5.3.d)] | [Test: AU-11(DHS-5.3.d) - Audit Log Retention]  Not Entered | Failure to meet the audit record retention requirements listed below could result in the loss of the generated audit data, which could render audit or forensic investigation efforts useless:  (i) audit logs are recorded and retained in accordance with the Component's Record Schedule or DHS Records Schedule;  (ii) audit trail records are maintained online for at least ninety (90) days; and,  (iii) audit trail records are preserved for a period of seven (7) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease. | High | [Test: AU-11(DHS-5.3.d) - Audit Log Retention]  Not Entered |  |
| [E-# OR W-#] | Collaborative Computing Devices [NIST 800-53 w/ DHS 4300A SC-15 (DHS-4.5.3.c)] | [Test: SC-15(DHS-4.5.3.c) - Disabling of Video Teleconference Software]  Not Entered | Failure to ensure that video teleconferencing equipment and software are disabled when not in use could allow the disclosure of critical DHS information. | High | [Test: SC-15(DHS-4.5.3.c) - Disabling of Video Teleconference Software]  Not Entered |  |
| [E-# OR W-#] | Contingency Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A CP-1 (DHS-3.5.2.d)] | [Test: CP-1(DHS-3.5.2.d) - DHS Contingency Guidance]  Not Entered | Failure to ensure contingency capabilities for DHS systems could result in the continued operation of the system, risking further loss or damage, or the removal of the system, causing functional outage for all authorized users. | High | [Test: CP-1(DHS-3.5.2.d) - DHS Contingency Guidance]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (12)] | [Test: IA-2(12).1 - Acceptance Of PIV Credentials]  Not Entered | Failure to meet the requirements of accepting PIV credentials listed below could result in providing any account access to critical or sensitive information:  (i) the information system accepts and electronically verifies Personal Identity Verification (PIV) credentials; (ii) the organization implements logical access control systems (LACS) and physical access control systems (PACS); and, (iii) the organization conforms to federal requirements when enabling agency-wide use of PIV credentials. | High | [Test: IA-2(12).1 - Acceptance Of PIV Credentials]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (DHS-5.5.3.c)] | [Test: SC-12(DHS-5.5.3.c) - Authorized Human Sponsor for DHS CA]  Not Entered | Failure to ensure that a human sponsor represented each application, role, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA could cause the organization to face litigations because of offenses related to non-compliance of these premises. | High | [Test: SC-12(DHS-5.5.3.c) - Authorized Human Sponsor for DHS CA]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5 (11)] | [Test: IA-5(11).1 - Hardware Token-Based Authentication]  Not Entered | Failure to employ organization-defined token quality requirement mechanisms to systems using hardware token-based authentication could leave the system vulnerable to unauthorized access, impersonation, and brute force attacks. | High | [Test: IA-5(11).1 - Hardware Token-Based Authentication]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.f)] | [Test: CA-3(DHS-5.4.3.f) - Interconnection Security Agreements]  Not Entered | Failure to meet the security requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization completes a master Interconnection Security Agreement (ISA) of all their transitioning systems as part of their initial OneNet transition;  (ii) the organization provides separate ISAs for every additional system or General Support System (GSS) after transition;  (iii) the organization requires an ISA whenever there is a difference in security categorizations for confidentiality, integrity and availability between systems or when systems do not share the same security policies; and,  (iv) the organization assigns the Authorizing Officer to sign the ISA. | High | [Test: CA-3(DHS-5.4.3.f) - Interconnection Security Agreements]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-3.7.f)] | [Test: CM-6(DHS-3.7.f) - USGCB Compliance]  Not Entered | Failure to monitor USGCB (or DHS-approved USGCB variant) compliance using a (NIST)-validated Security Content Automation Protocol (SCAP) tool could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or of systems that need configuration updates. | High | [Test: CM-6(DHS-3.7.f) - USGCB Compliance]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8 (3)] | [Test: IA-8(3).1 - Use Of FICAM-Approved Products]  Not Entered | Failure to ensure that the organization employs only FICAM-approved information system components to accept third-party credentials could result in the loss of system integrity. | High | [Test: IA-8(3).1 - Use Of FICAM-Approved Products]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-4.4.1.a)] | [Test: SC-1(DHS-4.4.1.a) - Private Branch Exchange(PBX) Protections]  Not Entered | Failure of the components to provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX) could result in the inability of the key organization personnel to respond properly to an incident in a timely manner, which could lead to the disruption of critical mission/business functions, operations, and processes. | High | [Test: SC-1(DHS-4.4.1.a) - Private Branch Exchange(PBX) Protections]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (10)] | [Test: SA-4(10).1 - Use Of Approved Piv Products]  Not Entered | Failure to ensure that the organization employs only information technology products on the FIPS 201-approved products list for Personal Identity Verification (PIV) capability implemented within organizational information systems could lead to the compromise of the system or of the data in the system. | High | [Test: SA-4(10).1 - Use Of Approved Piv Products]  Not Entered |  |
| [E-# OR W-#] | Security Planning Policy and Procedures [NIST 800-53 w/ DHS 4300A PL-1 (DHS-3.14.5.c)] | [Test: PL-1(DHS-3.14.5.c) - Sensitive PII]  Not Entered | Failure to ensure that systems that, as part of routine business, remove Sensitive PII in the form of a CRE, e.g., routine system-to-system transmissions of data (routine CREs) are addressed associated risks in the Security Plan could result in the weak security stance of the organization due to the lack of awareness on the security planning policy and procedures. | High | [Test: PL-1(DHS-3.14.5.c) - Sensitive PII]  Not Entered |  |
| [E-# OR W-#] | System and Services Acquisition Policy and Procedures [NIST 800-53 w/ DHS 4300A SA-1 (DHS-3.3.a)] | [Test: SA-1(DHS-3.3.a) - Statements of Work]  Not Entered | Failure to ensure that all Statements of Work (SOW) and contract vehicles have identified and documented the specific security requirements for information system services and operations required of the contractor could lead to non-compliance with the entity’s policies, procedures, privacy requirements, agreements or contracts. | High | [Test: SA-1(DHS-3.3.a) - Statements of Work]  Not Entered |  |
| [E-# OR W-#] | System and Services Acquisition Policy and Procedures [NIST 800-53 w/ DHS 4300A SA-1 (DHS-3.2.g)] | [Test: SA-1(DHS-3.2.g) - Procurements Regarding HSPD-12]  Not Entered | Failure to ensure that the procurements for services and products involving facility or system access control are in accordance with DHS guidance regarding HSPD-12 implementation could result in the acquisition of a system/service that would expose the organization to various threats and exploits, which could cause the loss of critical mission/business assets or the disruption of organization operations, functions and services. | High | [Test: SA-1(DHS-3.2.g) - Procurements Regarding HSPD-12]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.c)] | [Test: CA-3(DHS-5.4.3.c) - DHS OneNet Interconnections]  Not Entered | Failure to meet the security requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization maintains Interconnection Security Agreements (ISAs) for all connections between systems that do not have the same security policy; and,  (ii) the ISAs are authorized by the DHS OneNet Authorizing Officer. | High | [Test: CA-3(DHS-5.4.3.c) - DHS OneNet Interconnections]  Not Entered |  |
| [E-# OR W-#] | System and Services Acquisition Policy and Procedures [NIST 800-53 w/ DHS 4300A SA-1 (DHS-3.3.b)] | [Test: SA-1(DHS-3.3.b) - Contractor Information System Services and Operations]  Not Entered | Failure to ensure that the contractor information system services and operations adhere to all applicable DHS information security policies could result in the loss of system integrity and stability, which could lead to the disclosure of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SA-1(DHS-3.3.b) - Contractor Information System Services and Operations]  Not Entered |  |
| [E-# OR W-#] | Position Categorization [NIST 800-53 w/ DHS 4300A PS-2] | [Test: PS-2.1 - Position Risk Designation]  Not Entered | Failure to meet the position risk designation requirements indicated below could result in data compromise:  (i) the organization assigns a risk designation to all positions within the organization; (ii) the organization establishes a screening criteria for individuals filling organizational positions; and (iii) the organization defines the frequency of risk designation reviews and updates for organizational positions. | High | [Test: PS-2.1 - Position Risk Designation]  Not Entered |  |
| [E-# OR W-#] | System and Information Integrity Policy and Procedures [NIST 800-53 w/ DHS 4300A SI-1 (DHS-5.4.5.c)] | [Test: SI-1(DHS-5.4.5.c) - Use of Executable Code]  Not Entered | Failure of the components to ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment could result in the inability to detect threats/vulnerabilities and exploits identified with and inherent in malicious codes enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-1(DHS-5.4.5.c) - Use of Executable Code]  Not Entered |  |
| [E-# OR W-#] | Security Assessments [NIST 800-53 w/ DHS 4300A CA-2 (DHS-3.18.b)] | [Test: CA-2(DHS-3.18.b) - Cloud Systems Provided to External Departments]  Not Entered | Failure to meet the requirements for cloud systems provided to external departments listed below could result in a weak security stance of the organization due to security threats that may not have been addressed accordingly or completely by organizational personnel with certification, accreditation and assessment roles and responsibilities:   * all DHS cloud services intended for use by other departments and agencies are assessed by a Third Party Assessment Organization (3PAO); * all 3PAOs are accredited using a process that follows the conformity assessment approach outlined in ISO/IEC 17020, General Criteria for the operation of various types of bodies performing inspection (1998). | High | [Test: CA-2(DHS-3.18.b) - Cloud Systems Provided to External Departments]  Not Entered |  |
| [E-# OR W-#] | Security Assessment and Authorization Policies and Procedures [NIST 800-53 w/ DHS 4300A CA-1 (DHS-3.18.d)] | [Test: CA-1(DHS-3.18.d) - Usage of FedRAMP for Cloud Systems]  Not Entered | Failure to meet the FedRAMP cloud usage environment requirements listed below could result in a weak security stance of the organization due to security threats that may not have been addressed accordingly or completely by organizational personnel with certification, accreditation and assessment roles and responsibilities:   * the organization hosts DHS cloud services whether in DHS centers or in FedRAMP cloud service providers (CSP); * the organization allows all existing DHS cloud services undergo cloud usage assessment procedures:   (i) Assessment does not require a third-party assessment organizations (3PAOs) but shall use FedRAMP documentation templates. (ii) Assessment is done using existing processes. (iii) Assessment is categorized in the FISMA inventory as either a major application, minor application or subsystem. | High | [Test: CA-1(DHS-3.18.d) - Usage of FedRAMP for Cloud Systems]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan Testing and Exercises [NIST 800-53 w/ DHS 4300A CP-4] | [Test: CP-4.1 - Contingency Plan Testing]  Not Entered | Failure to meet the contingency plan testing and exercises requirements indicated below could lead to the unavailability of critical system resources and data due to the inability to restore the system or the data in a timely manner:  (i) the organization defines the contingency plan tests and/or exercises to be conducted; (ii) the organization defines the frequency of contingency plan tests and/or exercises; (iii) the organization tests/exercises the contingency plan using organization-defined tests/exercises in accordance with organization-defined frequency; and (iv) the organization reviews the contingency plan test/exercise results and takes corrective actions. | High | [Test: CP-4.1 - Contingency Plan Testing]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3] | [Test: CA-3.1 - System Interconnections]  Not Entered | Failure to meet the security requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization identifies connections to external information systems (i.e., information systems outside of the authorization boundary); (ii) the organization authorizes connections from the information system to external information systems through the use of Interconnection Security Agreements; (iii) the organization documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and (iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements. | High | [Test: CA-3.1 - System Interconnections]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (DHS-5.4.5.b)] | [Test: SC-7(DHS-5.4.5.b) - Configuration of Firewalls and PEPs]  Not Entered | Failure to ensure that firewalls and PEPs are configured to prohibit any protocol or service that is not explicitly permitted could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical DHS assets. | High | [Test: SC-7(DHS-5.4.5.b) - Configuration of Firewalls and PEPs]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13 (DHS-5.4.6.k)] | [Test: SC-13(DHS-5.4.6.k) - Unencrytped Email Usage]  Not Entered | Failure to ensure that the information sent outside the dhs.gov domain is encrypted could allow an attacker or a malicious user to perform information flooding types of denial of service attacks, which could lead to the compromise of the system or of the data in the system. | High | [Test: SC-13(DHS-5.4.6.k) - Unencrytped Email Usage]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7 (DHS-5.4.5.f)] | [Test: CM-7(DHS-5.4.5.f) - Remote Desktop Connections]  Not Entered | Failure to meet the requirements for configuration settings listed below could lead to the compromise of the system or of the data in the system:  (i) the organization does not authorize Remote Desktop connections (e.g. Microsoft's Remote Desktop Protocol) to any DHS computer without using secure authentication tools; and  (ii) the organization, upon authorizing RDP connections to any DHS computer, uses any of the following secure authentication methods:   * two factor * encrypted * key exchange | High | [Test: CM-7(DHS-5.4.5.f) - Remote Desktop Connections]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (DHS-4.1.2.a)] | [Test: PL-4(DHS-4.1.2.a) - DHS Rules of Behavior]  Not Entered | Failure to meet the rules of behavior requirements listed below could leave the users unaware of the required behavior with regard to information usage, which could lead to the user inadvertently abusing the information system resources:  (i) the components establish the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage; (ii) the components make the rules available to all information system users; and (iii) the components receive a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | High | [Test: PL-4(DHS-4.1.2.a) - DHS Rules of Behavior]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (DHS-5.5.3.a)] | [Test: SC-12(DHS-5.5.3.a) - DHS FPKI Human Subscriber]  Not Entered | Failure to ensure that a single public/private key pair is not used by a human subscriber for both encryption and digital signature could lead to the disclosure of critical DHS information/data. | High | [Test: SC-12(DHS-5.5.3.a) - DHS FPKI Human Subscriber]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.n)] | [Test: CA-3(DHS-5.4.3.n) - DHS Interconnections]  Not Entered | Failure to meet any of the requirements from Section 5.4.3 could lead to compromise of the system or of the data in the system. | High | [Test: CA-3(DHS-5.4.3.n) - DHS Interconnections]  Not Entered |  |
| [E-# OR W-#] | Access Records [NIST 800-53 w/ DHS 4300A PE-8] | [Test: PE-8.1 - Visitor Access Records]  Not Entered | Failure to meet the visitor access records requirements listed below could lead to the inadvertent disclosure of information:  (i) the organization maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and (ii) the organization defines the frequency to review visitor access records. | High | [Test: PE-8.1 - Visitor Access Records]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (DHS-4.8.3.a)] | [Test: PL-4(DHS-4.8.3.a) - Personally Owned Equipment]  Not Entered | Failure to ensure that personally owned equipment and software are used to process, access, or store sensitive information with the written prior approval of the AO could allow unauthorized user from executing critical transactions in DHS that can change application functionality. | High | [Test: PL-4(DHS-4.8.3.a) - Personally Owned Equipment]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7 (DHS-4.8.6.a)] | [Test: CM-7(DHS-4.8.6.a) - Wireless for Peripheral Equipment]  Not Entered | Failure to disable wireless capabilities of any peripheral equipment when connected to a DHS network or other IS containing sensitive data may result in unauthorized personnel gaining access and compromising or corrupting data. | High | [Test: CM-7(DHS-4.8.6.a) - Wireless for Peripheral Equipment]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication Policy and Procedures [NIST 800-53 w/ DHS 4300A IA-1 (DHS-3.14.7.c)] | [Test: IA-1(DHS-3.14.7.c) - E-Authentication]  Not Entered | Failure to meet the identification and authentication requirements listed below could weaken the overall security posture of the system due to lack of compliance to known standards and policies:  (i) the components implement the necessary guidelines for e-authentication requirements; and  (ii) the guidelines is in accordance with NIST SP 800-63, Electronic Authentication Guideline. | High | [Test: IA-1(DHS-3.14.7.c) - E-Authentication]  Not Entered |  |
| [E-# OR W-#] | Media Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A MP-1 (DHS-4.3.1.g)] | [Test: MP-1(DHS-4.3.1.g) - Protection of Printed Output]  Not Entered | Failure to meet requirements for media protection policy and procedures listed below could result in the users being unaware of the proper media protection or its extent, which could eventually lead to the organization losing critical mission/business assets in the form of unauthorized or unintentional disclosure of information:  (i) the users ensure the proper protection of printed output;  (ii) printing of sensitive documents is occur only when a trusted person is attending the printer. | High | [Test: MP-1(DHS-4.3.1.g) - Protection of Printed Output]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.b)] | [Test: CA-3(DHS-5.4.3.b) - Interconnection Establishment Procedures]  Not Entered | Failure to meet the security requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization identifies connections to non-DHS information systems (i.e., information systems outside of the authorization boundary);  (ii) the organization authorizes connections between DHS and non-DHS systems through the use of controlled interfaces and approved service providers;  (iii) the organization documents interagency agreements, memorandums of understanding, service level agreements or interconnection security agreements, whenever system connection is made with other Federal agencies; and,  (iv) the organization monitors the information system connections on an ongoing basis to verify enforcement of security requirements. | High | [Test: CA-3(DHS-5.4.3.b) - Interconnection Establishment Procedures]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (DHS-3.14.7.g)] | [Test: SA-4(DHS-3.14.7.g) - PIV Credentials]  Not Entered | Failure to ensure that all new systems under development are enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational could result in the acquisition of inherently unsafe/non-secure systems that would expose the organization to other exploits and threats/vulnerabilities, which could eventually lead to the loss of critical mission/business assets or to the disruption of DHS operations, functions and services. | High | [Test: SA-4(DHS-3.14.7.g) - PIV Credentials]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8 (1)] | [Test: IA-8(1).1 - Acceptance Of PIV Credentials From Other Agencies]  Not Entered | Failure to meet the requirements of accepting PIV credentials listed below could result in providing any account access to critical or sensitive information:  (i) the information system accepts and electronically verifies Personal Identity Verification (PIV) credentials from other federal agencies; (ii) the organization implements logical access control systems (LACS) and physical access control systems (PACS); and, (iii) the organization conforms to federal requirements when enabling agency-wide use of PIV credentials. | High | [Test: IA-8(1).1 - Acceptance Of PIV Credentials From Other Agencies]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication Policy and Procedures [NIST 800-53 w/ DHS 4300A IA-1 (DHS-1.6.d)] | [Test: IA-1(DHS-1.6.d) - PIV Credentials]  Not Entered | Failure to accept and verify PIV credentials by other Federal agencies as proof of identity could weaken the overall security posture of the system due to lack of compliance to known standards and policies. | High | [Test: IA-1(DHS-1.6.d) - PIV Credentials]  Not Entered |  |
| [E-# OR W-#] | Security Assessment and Authorization Policies and Procedures [NIST 800-53 w/ DHS 4300A CA-1 (DHS-3.18.e)] | [Test: CA-1(DHS-3.18.e) - Usage of Public Cloud Service Provider]  Not Entered | Failure to provide the proper documentation to the FedRAMP PMO regarding the existence of all DHS cloud services hosted in public CSPs could weaken the overall security posture of the system. | High | [Test: CA-1(DHS-3.18.e) - Usage of Public Cloud Service Provider]  Not Entered |  |
| [E-# OR W-#] | Continuous Monitoring [NIST 800-53 w/ DHS 4300A CA-7 (DHS-4.6.3.a)] | [Test: CA-7(DHS-4.6.3.a) - AO Notification on Disabling Security Features]  Not Entered | Failure to immediately notify AOs when any security features are disabled in response to time-sensitive, mission-critical incidents could render the security controls useless and outdated when examining recent or latest threat information and emerging vulnerabilities. | High | [Test: CA-7(DHS-4.6.3.a) - AO Notification on Disabling Security Features]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (DHS-5.4.4.h)] | [Test: SC-7(DHS-5.4.4.h) - Permitted Protocols and Services for Component PEPs]  Not Entered | Failure to meet the requirements listed below could lead to an attacker or a malicious user gaining unauthorized access to the system or data and could risk the loss of critical DHS assets.  (i) components determined protocols and services permitted through their Component-level PEPs. (ii) components may restrict traffic sources and destinations at their Component-level PEPs. | High | [Test: SC-7(DHS-5.4.4.h) - Permitted Protocols and Services for Component PEPs]  Not Entered |  |
| [E-# OR W-#] | Malicious Code Protection [NIST 800-53 w/ DHS 4300A SI-3 (10)] | [Test: SI-3(10).1 - Malicious Code Analysis]  Not Entered | Failure to meet the requirements for malicious code protection listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization employs organization-defined tools and techniques to analyze the characteristics and behavior of malicious code; and (ii) the organization incorporates the results from malicious code analysis into organizational incident response and flaw remediation processes. | High | [Test: SI-3(10).1 - Malicious Code Analysis]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan Testing and Exercises [NIST 800-53 w/ DHS 4300A CP-4 (DHS-3.5.2.f)] | [Test: CP-4(DHS-3.5.2.f) - DHS Contingency Plan Testing]  Not Entered | Failure to meet the contingency plan testing and exercises requirements indicated below could weaken the overall security posture of the system due to lack of compliance to known standards and policies:  (i) the DHS CIO performs CP testing in accordance with the availability security objective; and  (ii) the minimum contingency testing for each impact level follows:  High impact – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used within a year prior to authorization to recover from a simulated contingency event at the alternate processing site. The system recovery procedures in the CP shall be used at least annually to simulate system recovery in a test facility.  Moderate impact – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise.  Low impact – CP contact information shall be verified at least annually. | High | [Test: CP-4(DHS-3.5.2.f) - DHS Contingency Plan Testing]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (1)] | [Test: IA-2(1).1 - Network Access To Privileged Accounts]  Not Entered | Failure to ensure that the information system uses multifactor authentication for network access to privileged accounts could result in ineffective identification and authentication policy, which could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data. | High | [Test: IA-2(1).1 - Network Access To Privileged Accounts]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (DHS-5.4.1.c)] | [Test: AC-17(DHS-5.4.1.c) - Remote Access of PII]  Not Entered | Failure to employ strong authentication protocols to facilitate the monitoring and control of remote access methods for PII could result in a system breach through remote access attack vectors that could eventually lead to disclosure or compromise of high-level information. | High | [Test: AC-17(DHS-5.4.1.c) - Remote Access of PII]  Not Entered |  |
| [E-# OR W-#] | System and Information Integrity Policy and Procedures [NIST 800-53 w/ DHS 4300A SI-1 (DHS-5.4.6.h)] | [Test: SI-1(DHS-5.4.6.h) - Email Monitoring for Spam]  Not Entered | Failure to ensure that the DHS email gateway Steward provides email monitoring for spam at the gateway could result in the ineffective remediation strategy, which could eventually lead to the loss of sensitive information or to the disruption of critical DHS functions, services, and operations/processes. | High | [Test: SI-1(DHS-5.4.6.h) - Email Monitoring for Spam]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-4.12.f)] | [Test: CM-6(DHS-4.12.f) - Network Printers, Copiers, and Facsimile Administration]  Not Entered | Failure to ensure that the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to network printers, copiers, and facsimile machines could lead to the compromise of the system or of the data in the system. | High | [Test: CM-6(DHS-4.12.f) - Network Printers, Copiers, and Facsimile Administration]  Not Entered |  |
| [E-# OR W-#] | Denial-of-Service Protection [NIST 800-53 w/ DHS 4300A SC-5 (DHS-4.6.1.c)] | [Test: SC-5(DHS-4.6.1.c) - Denial of Service countermeasures]  Not Entered | Failure of the components to identify the countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of a wireless PED could result in non-secure system that lacks stability and integrity causing the unavailability of the system or the data in the system to authorized users. | High | [Test: SC-5(DHS-4.6.1.c) - Denial of Service countermeasures]  Not Entered |  |
| [E-# OR W-#] | Plan of Action and Milestones [NIST 800-53 w/ DHS 4300A CA-5 (DHS-2.2.8.d)] | [Test: CA-5(DHS-2.2.8.d) - DHS POA&M Requirements]  Not Entered | Failure to meet the plan of action and milestones requirements listed below exposes the system to security threats due to security holes that could have been patched in a timely manner, which could eventually lead to the compromise of the system or of the data in the system:  (i) the organization develops a plan of action and milestones for the information system;  (ii) the plan of action and milestones addresses the following:   * Known vulnerabilities in the information system. * Security categorization of the information system. * Specific weaknesses or deficiencies in the information system controls. * Importance of the identified security control weakness or deficiencies. * Component's proposed risk mitigation approach while addressing the identified weaknesses or deficiencies in the security controls and the rationale for accepting certain weaknesses or deficiencies in the security controls. | High | [Test: CA-5(DHS-2.2.8.d) - DHS POA&M Requirements]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (DHS-4.6.b)] | [Test: SC-12(DHS-4.6.b) - PKI Based Encryption]  Not Entered | Failure to ensure that the components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems implemented and maintained a key management plan approved by the DHS PKI Policy Authority could lead to the disclosure of critical DHS information/data. | High | [Test: SC-12(DHS-4.6.b) - PKI Based Encryption]  Not Entered |  |
| [E-# OR W-#] | Security Categorization [NIST 800-53 w/ DHS 4300A RA-2 (DHS-3.9.a)] | [Test: RA-2(DHS-3.9.a) - Security Objective Impact Level]  Not Entered | Failure to meet the security categorization listed below could result in ineffective controls and increased information security risks.  (i) components assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system; and (ii) components apply NIST SP800-53 controls as tailored in the DHS 4300A, Sensitive Systems Handbook, Attachment M specific to the security objective at the determined impact level. | High | [Test: RA-2(DHS-3.9.a) - Security Objective Impact Level]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (DHS-5.4.3.m)] | [Test: CA-3(DHS-5.4.3.m) - Interconnection Security Agreements]  Not Entered | Failure to meet the security requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization identifies interconnections between two authorized DHS systems;  (ii) the organization documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated, and monitoring procedures for verifying enforcement of security requirements; and,  (iii) the organization does not require an ISA if the interface characteristics, security requirements, the nature of the information communicated, and the monitoring procedures for verifying enforcement of security requirements are documented either in the Security Policy or other relevant formal document. | High | [Test: CA-3(DHS-5.4.3.m) - Interconnection Security Agreements]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-3.7.g)] | [Test: CM-6(DHS-3.7.g) - Hardening and Configuration Guidance]  Not Entered | Failure to meet the configuration requirements listed below could weaken the overall security posture of the system due to lack of compliance to known standards and policies:  (i) the system owner requests an exception for information systems or applications that are not hardened or do not follow configuration guidance as required; and  (ii) the request includes propsed alternative secure configurations. | High | [Test: CM-6(DHS-3.7.g) - Hardening and Configuration Guidance]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (DHS-4.8.5.e)] | [Test: PL-4(DHS-4.8.5.e) - Signed Rules of Behavior]  Not Entered | Failure to meet the rules of behavior requirements listed below could leave the users unaware of the required behavior with regard to information usage, which could lead to the user inadvertently abusing the information system resources:  (i) the components establish the rules that describe information system user responsibilities and expected behavior with regard to information and information system usage; (ii) the components make the rules available to all information system users; and (iii) the components receive a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system. | High | [Test: PL-4(DHS-4.8.5.e) - Signed Rules of Behavior]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5 (DHS-5.1.e)] | [Test: IA-5(DHS-5.1.e) - User Authentication Materials]  Not Entered | Failure to meet the user authentication material requirements listed below could leave the system vulnerable to unauthorized access, impersonation, and brute force attacks:  (i) all user authentication materials are treated as sensitive material; and, (ii) all user authentication materials treated as sensitive material carry a classification as high as the most sensitive data to which that user is granted access using that authenticator. | High | [Test: IA-5(DHS-5.1.e) - User Authentication Materials]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13] | [Test: SC-13.1 - Cryptographic Protection]  Not Entered | Failure to ensure that the information system implements organization-defined cryptographic uses and type of cryptography required for each use in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards could cause the organization to face litigations because of offenses related to non-compliance of these premises. | High | [Test: SC-13.1 - Cryptographic Protection]  Not Entered |  |
| [E-# OR W-#] | Media Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A MP-1 (DHS-5.6.c)] | [Test: MP-1(DHS-5.6.c) - Media Scanning]  Not Entered | Failure of the System Owners to manage malicious code protection mechanisms and proper malware scanning mechanisms could result in the inability to detect threats/vulnerabilities and exploits identified with and inherent in malicious codes enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: MP-1(DHS-5.6.c) - Media Scanning]  Not Entered |  |
| [E-# OR W-#] | System and Information Integrity Policy and Procedures [NIST 800-53 w/ DHS 4300A SI-1 (DHS-5.4.2.a)] | [Test: SI-1(DHS-5.4.2.a) - Continuous Monitoring of Networks]  Not Entered | Failure to ensure that the components provide continuous monitoring of their network for security events or outsource this requirement to the DHS EOC could result in the ineffective system and information integrity policy, which could eventually lead to the loss of sensitive information or to the disruption of critical DHS functions, services, and operations/processes. | High | [Test: SI-1(DHS-5.4.2.a) - Continuous Monitoring of Networks]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13 (DHS-5.5.1.c)] | [Test: SC-13(DHS-5.5.1.c) - Encryption Compliance with FIPS 197 and FIPS 140-2]  Not Entered | Failure of the components to use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their use could lead to the organization to face litigations because of offenses related to non-compliance of these premises. | High | [Test: SC-13(DHS-5.5.1.c) - Encryption Compliance with FIPS 197 and FIPS 140-2]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (DHS-5.1.d)] | [Test: IA-2(DHS-5.1.d) - Usage of Identification or Authentication Materials]  Not Entered | Failure to meet the requirements for using identification or authentication materials listed below could expose information system to unauthorized access and lead to compromise of information system integrity and confidentiality:  (i) use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment; and, (ii) use of a group User ID and password shall be approved by the appropriate Authorizing Official (AO). | High | [Test: IA-2(DHS-5.1.d) - Usage of Identification or Authentication Materials]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-4.8.4.a)] | [Test: CM-6(DHS-4.8.4.a) - Hardening and Configuration Guidance]  Not Entered | Failure to ensure that the information system (including modifications to the baseline configuration) demonstrates conformance to security configuration guidance, could weaken the overall security posture of the system due to lack of compliance to known standards and policies. | High | [Test: CM-6(DHS-4.8.4.a) - Hardening and Configuration Guidance]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-3.17.a)] | [Test: SC-1(DHS-3.17.a) - HIPAA Compliance]  Not Entered | Failure to ensure that the components whose systems collect, process, or store Protected Health Information (PHI) is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required could allow any personnel to obtain unauthorized or inappropriate access to applications and application data. | High | [Test: SC-1(DHS-3.17.a) - HIPAA Compliance]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5 (1)] | [Test: IA-5(1).1 - Password-Based Authentication]  Not Entered | Failure to meet the authenticator management requirements listed below could leave the system vulnerable to unauthorized access, impersonation, and brute force attacks:  (i) the organization defines the minimum password complexity requirements to be enforced for case sensitivity, the number of characters, and the mix of upper-case letters, lower-case letters, numbers, and special characters including minimum requirements for each type; (ii) the organization defines the minimum number of characters that must be changed when new passwords are created; (iii) the organization defines the restrictions to be enforced for password minimum lifetime and password maximum lifetime parameters; (iv) the organization defines the number of generations for which password reuse is prohibited; and (v) the information system, for password-based authentication:   * enforces the minimum password complexity standards that meet the organization-defined requirements; * enforces the organization-defined minimum number of characters that must be changed when new passwords are created; * encrypts passwords in storage and in transmission; * enforces the organization-defined restrictions for password minimum lifetime and password maximum lifetime parameters; and * prohibits password reuse for the organization-defined number of generations. | High | [Test: IA-5(1).1 - Password-Based Authentication]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (DHS-3.5.2.e)] | [Test: CP-2(DHS-3.5.2.e) - DHS Contingency Plan]  Not Entered | Failure to meet the contingency plan requirements listed below could lead to the unavailability of systems that is critical to the overall business processes:  (i) the DHS components develop and maintain Contingency Plans;  (ii) Contigency Plans are based on three essential phases: Activation/Notification, Recovery, and Reconstitution; and  (iii) the DHS Components review Contingency Plans at least annually and revises it in order to address system/organizational changes/problems encountered during the implementation, execution, or testing phase. | High | [Test: CP-2(DHS-3.5.2.e) - DHS Contingency Plan]  Not Entered |  |
| [E-# OR W-#] | Physical and Environmental Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A PE-1 (DHS-3.3.c)] | [Test: PE-1(DHS-3.3.c) - Sensitive Information at Contractor Sites]  Not Entered | Failure to meet the requirements for physical and environmental protection policy and procedures listed below could lead to the loss or modification of critical data, disruption of services, and/or the compromise of proprietary plans or processes:  (i) address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems;  (ii) include requirements for personnel background investigations and clearances, and facility security. | High | [Test: PE-1(DHS-3.3.c) - Sensitive Information at Contractor Sites]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8 (4)] | [Test: IA-8(4).1 - Use Of Ficam-Issued Profiles]  Not Entered | Failure to ensure that the information system conforms to FICAM-issued profiles could weaken its security posture, resulting to the ineffectiveness of the identification and authentication policy. | High | [Test: IA-8(4).1 - Use Of Ficam-Issued Profiles]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-5.7.a)] | [Test: SC-1(DHS-5.7.a) - Information Assurance Considerations]  Not Entered | Failure to meet the requirements below could lead to ineffectively remediate information security weaknesses:  (i) Information Assurance (IA) is considered a requirement for all systems used to input, process, store, display, or transmits sensitive or national security information.  (ii) IA is achieved through the acquisition and appropriate implementation of evaluated or validated commercial off-the-shelf (COTS) IA and IA-enabled IT products.  (iii) The products are provided for the availability of systems. (iv) The products ensured the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions. | High | [Test: SC-1(DHS-5.7.a) - Information Assurance Considerations]  Not Entered |  |
| [E-# OR W-#] | Access Enforcement [NIST 800-53 w/ DHS 4300A AC-3 (DHS-5.1.1.d)] | [Test: AC-3(DHS-5.1.1.d) - Use of group passwords]  Not Entered | Failure to meet the requirements for using group IDs listed below could expose the information system to unauthorized access and lead to compromise of the system's integrity and confidentiality:   * group passwords are limited to situations dictated by operational necessity or critical for mission accomplishment; and, * group User ID and password is approved by the appropriate Authorizing Official (AO). | High | [Test: AC-3(DHS-5.1.1.d) - Use of group passwords]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (DHS-5.4.5.a)] | [Test: SC-7(DHS-5.4.5.a) - Connection through TIC PEPs]  Not Entered | Failure to meet the boundary protection requirements listed below could lead to unauthorized access to the system or data being undetected in a timely manner and could risk the loss of critical DHS assets:  (i) Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets are occurring through DHS Trusted Internet Connection (TIC) PEPs.  (ii) The PSTN is not connected to OneNet at any time. | High | [Test: SC-7(DHS-5.4.5.a) - Connection through TIC PEPs]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-4.5.2.b)] | [Test: CM-6(DHS-4.5.2.b) - FAX Server Configuration]  Not Entered | Failure to configure secure incoming lines for fax servers may result in data being intercepted or compromised. | High | [Test: CM-6(DHS-4.5.2.b) - FAX Server Configuration]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (DHS-4.8.2.b)] | [Test: PL-4(DHS-4.8.2.b) - Laptop Power Down]  Not Entered | Failure to ensure that the computers are powered down when not in use (due to volatile memory vulnerabilities) could lead to computer resources damaged or destroyed. | High | [Test: PL-4(DHS-4.8.2.b) - Laptop Power Down]  Not Entered |  |
| [E-# OR W-#] | Media Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A MP-1 (DHS-5.4.1.d)] | [Test: MP-1(DHS-5.4.1.d) - PII Remote Access]  Not Entered | Failure to meet the media protection policy and procedures requirements indicated below could lead to the compromise of the system or of the data in the system:  (i) remote access of PII does not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed;  (ii) all downloads follow the concept of least privilege and are documented with the Security Plan. | High | [Test: MP-1(DHS-5.4.1.d) - PII Remote Access]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (DHS-4.12.j)] | [Test: CM-6(DHS-4.12.j) - Multifunction Device Configuration]  Not Entered | Failure to disable the inbound dial-in capabilities of any multifunction device when connected to a DHS network or other IS containing sensitive data may result in unauthorized personnel gaining access and compromising or corrupting data. | High | [Test: CM-6(DHS-4.12.j) - Multifunction Device Configuration]  Not Entered |  |
| [E-# OR W-#] | Use of Cryptography [NIST 800-53 w/ DHS 4300A SC-13 (DHS-5.5.2.v)] | [Test: SC-13(DHS-5.5.2.v) - Cryptography for Commerical Products]  Not Entered | Failure to ensure that the commercial products used by DHS and applications developed by DHS that enable the use of PKI are at a minimum support the following cryptographic algorithms and associated key sizes could cause the organization to face litigations because of offenses related to non-compliance of these premises:   * SHA 1 * SHA 256 * RSA with 1024 Bit keys * RSA with 2048 bit keys * AES 128 * AES 256 | High | [Test: SC-13(DHS-5.5.2.v) - Cryptography for Commerical Products]  Not Entered |  |
| [E-# OR W-#] | System and Communications Protection Policy and Procedures [NIST 800-53 w/ DHS 4300A SC-1 (DHS-5.5.2.t)] | [Test: SC-1(DHS-5.5.2.t) - Use of PKI]  Not Entered | Failure to meet the requirements for using PKI listed below could lead to non-compliance with the entity’s policies, procedures, privacy requirements, agreements or contracts:  (i ) the organization ensures that commercial applications or appliances used by DHS that require the use of PKI certificates obtain their certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate.  (ii) the organization ensures that commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, are not acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained. | High | [Test: SC-1(DHS-5.5.2.t) - Use of PKI]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Non-Organizational Users) [NIST 800-53 w/ DHS 4300A IA-8 (DHS-1.5.4.c)] | [Test: IA-8(DHS-1.5.4.c) - Foreign Nationals]  Not Entered | Failure to maitain additional compensating controls for foreign nationals could leave the system vulnerable to unauthorized access and intrusion. | High | [Test: IA-8(DHS-1.5.4.c) - Foreign Nationals]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5 (DHS-4.8.4.d)] | [Test: RA-5(DHS-4.8.4.d) - ISVM Compliance]  Not Entered | Failure of the components to manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services could result in weaker security posture, which could lead to unauthorized disclosure of more information. | High | [Test: RA-5(DHS-4.8.4.d) - ISVM Compliance]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (DHS-5.5.3.b)] | [Test: SC-12(DHS-5.5.3.b) - PKI for NPE]  Not Entered | Failure to ensure that a single public/private key pair is not used by an NPE for both encryption and digital signature, whenever their separate use is supported by the protocols native to the NPE could lead to the disclosure of critical DHS information/data. | High | [Test: SC-12(DHS-5.5.3.b) - PKI for NPE]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (DHS-5.5.3.i)] | [Test: SC-12(DHS-5.5.3.i) - Subscriber Use of Private Key]  Not Entered | Failure to meet the subscriber use of private key requirements listed below could lead to the organization to face litigations because of offenses related to non-compliance:  If subscriber private keys are not be used by more than one entity, then the organization should abide to the following exceptions:  • authorized members of a Group Subscriber, may use the Group’s private keys; and  • multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared. | High | [Test: SC-12(DHS-5.5.3.i) - Subscriber Use of Private Key]  Not Entered |  |
| [E-# OR W-#] | Non-Local Maintenance [NIST 800-53 w/ DHS 4300A MA-4] | [Test: MA-4.1 - Nonlocal Maintenance]  Not Entered | Failure to meet the non-local maintenance requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization authorizes, monitors, and controls non-local maintenance and diagnostic activities; (ii) the organization documents, in the organizational policy and security plan for the information system, the acceptable conditions for allowing the use of non-local maintenance and diagnostic tools; (iii) the organization allows the use of non-local maintenance and diagnostic tools only as consistent with organizational policy and as documented in the security plan;  (iv) the organization employs strong identification and authentication techniques in the establishment of non-local maintenance and diagnostic sessions; (v) the organization maintains records for non-local maintenance and diagnostic activities; and (vi) the organization (or information system in certain cases) terminates all sessions and network connections when non-local maintenance or diagnostics is completed. | High | [Test: MA-4.1 - Nonlocal Maintenance]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7 (2)] | [Test: CM-7(2).1 - Prevent Program Execution]  Not Entered | Failure to meet the least functionality requirements listed below could leave the system vulnerable to attacks and denial of service conditions:  (i) the organization develops and maintains one or more of the following specifications to prevent software program execution on the information system:   * a list of software programs authorized to execute on the information system; * a list of software programs not authorized to execute on the information system; and/or * rules authorizing the terms and conditions of software program usage on the information system; and   (ii) the organization employs automated mechanisms to prevent software program execution on the information system in accordance with the organization-defined specifications. | High | [Test: CM-7(2).1 - Prevent Program Execution]  Not Entered |  |
| [E-# OR W-#] | Configuration Change Control [NIST 800-53 w/ DHS 4300A CM-3 (2)] | [Test: CM-3(2).1 - Test / Validate / Document Changes]  Not Entered | Failure to ensure that the organization tests, validates, and documents changes to the information system before implementing the changes on the operational system could leave the system vulnerable to unexpected crashes or instability in operation. | High | [Test: CM-3(2).1 - Test / Validate / Document Changes]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (7)] | [Test: CM-2(7).1 - Configure Systems, Components, Or Devices For High-Risk Areas]  Not Entered | Failure to meet the baseline configuration requirements listed below could result in a system that is not properly configured or with a weak security stance, which could lead to the compromise of data or the system itself:  (i) the organization issues information systems, system components, or devices with secured configurations to individuals travelling to locations that the organization deems to be of significant risk; and, (ii) the organization applies security safeguards to the devices when the individuals return. | High | [Test: CM-2(7).1 - Configure Systems, Components, Or Devices For High-Risk Areas]  Not Entered |  |
| [E-# OR W-#] | Session Lock [NIST 800-53 w/ DHS 4300A AC-11] | [Test: AC-11.1 - Session Lock]  Not Entered | Failure to meet session lock requirements indicated below could enable an attacker to try and break into the system by hijacking the idle session:  (i) the organization defines the time period of user inactivity after which the information system initiates a session lock; and, (ii) the information system retains the session lock until the user reestablishes access using established identification and authentication procedures. | High | [Test: AC-11.1 - Session Lock]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (5)] | [Test: SI-7(5).1 - Automated Response To Integrity Violations]  Not Entered | Failure to ensure that the information system automatically shuts the information system down, restarts the information system, or implements organization-defined security safeguards when integrity violations are discovered could result in the untimely remediation of discrepancies on/of information system functionality, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-7(5).1 - Automated Response To Integrity Violations]  Not Entered |  |
| [E-# OR W-#] | Protection of Information at Rest [NIST 800-53 w/ DHS 4300A SC-28] | [Test: SC-28.1 - Protection of Information at Rest]  Not Entered | Failure to ensure that the information system protects the confidentiality and integrity of information at rest could risk the disclosure of sensitive information or the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SC-28.1 - Protection of Information at Rest]  Not Entered |  |
| [E-# OR W-#] | Configuration Management Plan [NIST 800-53 w/ DHS 4300A CM-9] | [Test: CM-9.1 - Configuration Management Plan]  Not Entered | Failure to meet the configuration management plan requirements listed below could weaken the overall security posture of the system:  (i) the organization develops, documents, and implements a configuration management plan for the information system that:   * addresses roles, responsibilities, and configuration management processes and procedures; * defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and * establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items. | High | [Test: CM-9.1 - Configuration Management Plan]  Not Entered |  |
| [E-# OR W-#] | Information System Backup [NIST 800-53 w/ DHS 4300A CP-9 (5)] | [Test: CP-9(5).1 - Transfer To Alternate Storage Site]  Not Entered | Failure to meet the information system backup requirements listed below could cause the loss of essential data in the event of an attack:  (i) the organization defines the time period and rate of transferring information system backup information to the alternate storage site to support recovery time objectives and recovery point objectives; and (ii) the organization transfers information system backup information to the alternate storage site in accordance with the organization-defined frequency and transfer rate. | High | [Test: CP-9(5).1 - Transfer To Alternate Storage Site]  Not Entered |  |
| [E-# OR W-#] | Security Assessments [NIST 800-53 w/ DHS 4300A CA-2 (2)] | [Test: CA-2(2).1 - Specialized Assessments]  Not Entered  [Test: CA-2.2 - Security Assessments]  Not Entered | Failure to meet the security assessments requirements listed below could weaken the overall security posture of the system:  (i) the organization defines the frequency of assessing the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; (ii) the organization assesses the security controls in the information system at the organization-defined frequency; (iii) the organization produces a security assessment report that documents the results of the security control assessment; and (iv) the results of the security control assessment are provided, in writing, to the authorizing official or authorizing official designated representative.  Failure to meet the security assessments requirements listed below could weaken the overall security posture of the system:  (i) the organization defines:   * the forms of security testing to be included in security control assessments, selecting from in-depth monitoring, malicious user testing, penetration testing, red team exercises, or an organization-defined form of security testing; * the frequency for conducting each form of security testing; * whether the security testing will be announced or unannounced; and   (ii) the organization conducts security control assessments using organization-defined forms of testing in accordance with organization-defined frequency and assessment techniques established for each form of testing. | High | [Test: CA-2(2).1 - Specialized Assessments]  Not Entered  [Test: CA-2.2 - Security Assessments]  Not Entered |  |
| [E-# OR W-#] | Protection of Information at Rest [NIST 800-53 w/ DHS 4300A SC-28 (DHS-5.2.g)] | [Test: SC-28(DHS-5.2.g) - DHS Data at Rest Requirements]  Not Entered | Failure of the components and programs to ensure that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the data storage) could risk the disclosure of sensitive information or the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SC-28(DHS-5.2.g) - DHS Data at Rest Requirements]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (DHS-4.12.b)] | [Test: CM-2(DHS-4.12.b) - Network Printers and Facsimile Machines]  Not Entered | Failure of the organization to employ automated mechanisms to ensure network printers and facsimile machines are up-to-date with the latest software version/firmware could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or of systems that need configuration updates. | High | [Test: CM-2(DHS-4.12.b) - Network Printers and Facsimile Machines]  Not Entered |  |
| [E-# OR W-#] | Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7] | [Test: CP-7.1 - Alternate Processing Site]  Not Entered | Failure to meet the requirements for alternate processing site indicated below could lead to the interruption of business processes:  (i) the organization establishes an alternate processing site; (ii) the organization defines the time period for achieving the recovery time objectives within which processing must be resumed at the alternate processing site; (iii) the organization includes necessary alternate processing site agreements to permit the resumption of information system operations for essential missions and business functions within organization-defined time period; and (iv) the equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. | High | [Test: CP-7.1 - Alternate Processing Site]  Not Entered |  |
| [E-# OR W-#] | Security Functionality Verification [NIST 800-53 w/ DHS 4300A SI-6] | [Test: SI-6.1 - Security Function Verification]  Not Entered | Failure to meet the requirements for security functionality verification listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization verifies the correct operation of organization-defined security functions; (ii) the organization performs this verification organization-defined system transitional states, upon command by user with appropriate privilege or organization-defined frequency; (iii) the organization notifies organization-defined personnel or roles of failed automated security tests; and (iv) the organization shuts the information system down, restarts the information system or organization-defined alternative action(s) when anomalies are discovered. | High | [Test: SI-6.1 - Security Function Verification]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (1)] | [Test: AC-2(1).1 - Automated System Account Management]  Not Entered | Failure of the organization to employ automated mechanisms to support information system account management functions could promote a non-standard way of handling information system account management functions resulting in inaccurate information critical to the operation of the system. | High | [Test: AC-2(1).1 - Automated System Account Management]  Not Entered |  |
| [E-# OR W-#] | Access Control for Output Devices [NIST 800-53 w/ DHS 4300A PE-5] | [Test: PE-5.1 - Access Control for Output Devices]  Not Entered | Failure of the organization to control physical access to information system devices that display information to prevent unauthorized individuals from observing the display output could lead to the compromise of the system or of the data in the system. | High | [Test: PE-5.1 - Access Control for Output Devices]  Not Entered |  |
| [E-# OR W-#] | Use of External Information Systems [NIST 800-53 w/ DHS 4300A AC-20 (1)] | [Test: AC-20(1).1 - Limits On Authorized Use]  Not Entered | Failure to ensure that the organization prohibits authorized individuals from using an external information system to access the information system or to process, store, or transmit organization-controlled information except in situations listed below could result in a weaker security posture enabling would-be attackers to piggyback on personally owned information systems connected to the organization's own information system and extract vital corporate information and cause damage to the resources therein:   * the organization verifies the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or, * the organization retains information system connection or processing agreements with the organizational entity hosting the external information system. | High | [Test: AC-20(1).1 - Limits On Authorized Use]  Not Entered |  |
| [E-# OR W-#] | Network Disconnect [NIST 800-53 w/ DHS 4300A SC-10] | [Test: SC-10.1 - Network Disconnect]  Not Entered | Failure to ensure that the information system terminates the network connection associated with a communications session at the end of the session or after organization-defined time period of inactivity could lead to instability of the system brought about by unterminated inactive sessions. | High | [Test: SC-10.1 - Network Disconnect]  Not Entered |  |
| [E-# OR W-#] | Information Security Architecture [NIST 800-53 w/ DHS 4300A PL-8] | [Test: PL-8.1 - Information Security Architecture]  Not Entered | Failure to meet the information security architecture requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization develops an information security architecture for the information system that:   * describes the overall philosophy, requirements, and approach to be taken with regard to protecting the confidentiality, integrity, and availability of organizational information; * describes how the information security architecture is integrated into and supports the enterprise architecture; and * describes any information security assumptions about, and dependencies on, external services;   (ii) the organization defines the frequency of reviews and updates to the information security architecture to reflect updates in the enterprise architecture; and, (iii) the organization ensures that planned information security architecture changes are reflected in the security plan, the security Concept of Operations (CONOPS), and organizational procurements/acquisitions. | High | [Test: PL-8.1 - Information Security Architecture]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (3)] | [Test: AU-6(3).1 - Correlate Audit Repositories]  Not Entered | Failure to ensure that the organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness could prevent the proper implementation of standard audit requirements and protocols. | High | [Test: AU-6(3).1 - Correlate Audit Repositories]  Not Entered |  |
| [E-# OR W-#] | Information System Backup [NIST 800-53 w/ DHS 4300A CP-9 (1)] | [Test: CP-9(1).1 - Testing For Reliability / Integrity]  Not Entered | Failure to meet the information system backup requirements indicated below could result in the loss of data or of system integrity due to ineffective or untested backup process/reliability, which could lead to the disruption of critical mission/business functions, operations, and processes:   (i) the organization defines the frequency of information system backup testing; and (ii) the organization conducts information system backup testing in accordance with organization-defined frequency to verify backup media reliability and information integrity. | High | [Test: CP-9(1).1 - Testing For Reliability / Integrity]  Not Entered |  |
| [E-# OR W-#] | Information System Connections [NIST 800-53 w/ DHS 4300A CA-3 (5)] | [Test: CA-3(5).1 - Restrictions On External System Connections]  Not Entered | Failure to meet the external restriction connection requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization employs one of two policies with regard to information systems connecting to external domains:   * allow-all, deny by exception (or blacklisting); or, * deny-all, allow by exception (or whitelisting).   (ii) the organization determines the acceptable exceptions for allowing organization-defined information systems connecting to external information systems. | High | [Test: CA-3(5).1 - Restrictions On External System Connections]  Not Entered |  |
| [E-# OR W-#] | Configuration Change Control [NIST 800-53 w/ DHS 4300A CM-3] | [Test: CM-3.1 - Configuration Change Control]  Not Entered | Failure to meet the configuration change control requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization determines the types of changes to the information system that are configuration controlled; (ii) the organization approves configuration-controlled changes to the system with explicit consideration for security impact analyses; (iii) the organization documents approved configuration-controlled changes to the system; (iv) the organization retains and reviews records of configuration-controlled changes to the system; (v) the organization audits activities associated with configuration-controlled changes to the system; (vi) the organization defines:   * the configuration change control element (e.g., committee, board) responsible for coordinating and providing oversight for configuration change control activities; * the frequency with which the configuration change control element convenes; and/or; * configuration change conditions that prompt the configuration change control element to convene.   (vii) the organization coordinates and provides oversight for configuration change control activities through the organization-defined configuration change control element that convenes at the organization-defined frequency and/or for any organization-defined configuration change conditions. | High | [Test: CM-3.1 - Configuration Change Control]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (8)] | [Test: CP-2(8).1 - Identify Critical Assets]  Not Entered | Failure to ensure that the organization identifies critical information system assets supporting essential missions and business functions could lead to the unavailability of systems that is critical to the overall business processes. | High | [Test: CP-2(8).1 - Identify Critical Assets]  Not Entered |  |
| [E-# OR W-#] | Alternate Storage Site [NIST 800-53 w/ DHS 4300A CP-6 (3)] | [Test: CP-6(3).1 - Accessibility]  Not Entered | Failure to meet the alternate storage site requirements listed below could lead to the untimely recovery or restoration of system or of data:  (i) the organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster. | High | [Test: CP-6(3).1 - Accessibility]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (3)] | [Test: AC-17(3).1 - Managed Access Control Points]  Not Entered | Failure to meet the remote access requirements listed below could leave all data in transit vulnerable to unmonitored interception:  (i) the organization defines a limited number of managed access control points for remote access to the information system; and (ii) the information system routes all remote accesses through managed access control points. | High | [Test: AC-17(3).1 - Managed Access Control Points]  Not Entered |  |
| [E-# OR W-#] | Configuration Change Control [NIST 800-53 w/ DHS 4300A CM-3 (1)] | [Test: CM-3(1).1 - Automated Document / Notification / Prohibition Of Changes]  Not Entered | Failure to meet the configuration change control requirements listed below could allow any user to easily modify system configuration without being audited in a timely manner, which could lead to the loss of the integrity or stability of the system:  (i) the organization defines the time period after which approvals that have not been received for proposed changes to the information system are highlighted; and (ii) the organization employs automated mechanisms to:   * document proposed changes to the information system; * notify designated approval authorities; * highlight approvals that have not been received by the organization-defined time period; * inhibit change until designated approvals are received; and * document completed changes to the information system. | High | [Test: CM-3(1).1 - Automated Document / Notification / Prohibition Of Changes]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (18)] | [Test: SC-7(18).1 - Fail Secure]  Not Entered | Failure to ensure that the information system fails securely in the event of an operational failure of a boundary protection device could allow a hacker to gain control over an application. | High | [Test: SC-7(18).1 - Fail Secure]  Not Entered |  |
| [E-# OR W-#] | Audit Reduction and Report Generation [NIST 800-53 w/ DHS 4300A AU-7 (1)] | [Test: AU-7(1).1 - Automatic Processing]  Not Entered | Failure of the information system to provide the capability to automatically process audit records for events of interest based upon selectable event criteria could lead to the inability to track in a timely manner any attack on the system or data. | High | [Test: AU-7(1).1 - Automatic Processing]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (9)] | [Test: SA-4(9).1 - Functions / Ports / Protocols / Services In Use]  Not Entered | Failure to ensure that the organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use could eventually lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services. | High | [Test: SA-4(9).1 - Functions / Ports / Protocols / Services In Use]  Not Entered |  |
| [E-# OR W-#] | Flaw Remediation [NIST 800-53 w/ DHS 4300A SI-2 (2)] | [Test: SI-2(2).1 - Automated Flaw Remediation Status]  Not Entered | Failure to ensure that the organization employs automated mechanisms organization-defined frequency to determine the state of information system components with regard to flaw remediation could results in the untimely detection of the need to implement remediation strategy, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-2(2).1 - Automated Flaw Remediation Status]  Not Entered |  |
| [E-# OR W-#] | Concurrent Session Control [NIST 800-53 w/ DHS 4300A AC-10] | [Test: AC-10.1 - Concurrent Session Control]  Not Entered | Failure to meet the concurrent session control requirements listed below could enable an attacker to try and break into the system by hijacking the session and cause damage to the information system:  (i) the organization defines the maximum number of concurrent sessions to be allowed for each system account; and (ii) the information system limits the number of concurrent sessions for each system account to the organization-defined number of sessions. | High | [Test: AC-10.1 - Concurrent Session Control]  Not Entered |  |
| [E-# OR W-#] | Spam Protection [NIST 800-53 w/ DHS 4300A SI-8 (2)] | [Test: SI-8(2).1 - Automatic Updates]  Not Entered | Failure of the information system to automatically update spam protection mechanisms leaves the organization with an ineffective information system, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-8(2).1 - Automatic Updates]  Not Entered |  |
| [E-# OR W-#] | External Information System Services [NIST 800-53 w/ DHS 4300A SA-9 (2)] | [Test: SA-9(2).1 - Identification Of Functions / Ports / Protocols / Services]  Not Entered | Failure to ensure that the organization requires providers of organization-defined external information system services to identify the functions, ports, protocols, and other services required for the use of such services could eventually lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services. | High | [Test: SA-9(2).1 - Identification Of Functions / Ports / Protocols / Services]  Not Entered |  |
| [E-# OR W-#] | Incident Response Training [NIST 800-53 w/ DHS 4300A IR-2 (2)] | [Test: IR-2(2).1 - Automated Training Environments]  Not Entered | Failure of the organization to employ automated incident response training mechanisms to provide a more thorough and realistic training environment could result in the inability to respond properly to an incident, which could lead to the disruption of critical mission/business functions, operations, and processes. | High | [Test: IR-2(2).1 - Automated Training Environments]  Not Entered |  |
| [E-# OR W-#] | Power Equipment and Power Cabling [NIST 800-53 w/ DHS 4300A PE-9] | [Test: PE-9.1 - Power Equipment and Cabling]  Not Entered | Failure of the organization to protect power equipment and power cabling for the information system from damage and destruction could cause the unavailability of several system functionalities or information contained in the system. | High | [Test: PE-9.1 - Power Equipment and Cabling]  Not Entered |  |
| [E-# OR W-#] | Telecommunications Services [NIST 800-53 w/ DHS 4300A CP-8] | [Test: CP-8.1 - Telecommunications Services]  Not Entered | Failure to meet the telecommunication services requirements listed below could affect the timely resumption of telecommunication services for critical mission/business functions when the primary telecommunications capabilities are unavailable:  (i) the organization establishes alternate telecommunications services to support the information system; (ii) the organization defines in the time period within which resumption of information system operations must take place; and (iii) the organization establishes necessary alternate telecommunications service agreements to permit the resumption of telecommunications services for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable. | High | [Test: CP-8.1 - Telecommunications Services]  Not Entered |  |
| [E-# OR W-#] | Information System Monitoring [NIST 800-53 w/ DHS 4300A SI-4 (5)] | [Test: SI-4(5).1 - System-Generated Alerts]  Not Entered | Failure to to ensure that the information system alerts organization-defined personnel or roles when the following indications of compromise or potential compromise occur.could result in the inability to respond to any attack on, intrusion of or unusual/unauthorized use of the information system enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-4(5).1 - System-Generated Alerts]  Not Entered |  |
| [E-# OR W-#] | Audit Generation [NIST 800-53 w/ DHS 4300A AU-12 (1)] | [Test: AU-12(1).1 - System-Wide / Time-Correlated Audit Trail]  Not Entered | Failure to meet the audit generation requirements listed below could result in the loss of the generated audit data, which could render an audit or forensic investigation efforts useless:  (i) the organization defines the information system components from which audit records are to be compiled into the system-wide audit trail; (ii) the information system compiles audit records from organization-defined information system components into the system-wide audit trail; (iii) the organization defines the acceptable level of tolerance for relationship between time stamps of individual records in the system-wide audit trail; and, (iv) the system-wide audit trail is time-correlated to within the organization-defined level of tolerance to achieve a time ordering of audit records. | High | [Test: AU-12(1).1 - System-Wide / Time-Correlated Audit Trail]  Not Entered |  |
| [E-# OR W-#] | Non-Local Maintenance [NIST 800-53 w/ DHS 4300A MA-4 (3)] | [Test: MA-4(3).1 - Comparable Security / Sanitization]  Not Entered | Failure to ensure that the organization does not allow remote diagnostic or maintenance services to be performed by a provider that does not implement for its own information system, a level of security at least as high as the level of security implemented on the information system being serviced, unless the component being serviced is removed from the information system and sanitized (with regard to organizational information) before the service begins and also sanitized (with regard to potentially malicious software) after the service is performed and before being reconnected to the information system, could result in the system losing its integrity and stability or in the critical information/data being disclosed. | High | [Test: MA-4(3).1 - Comparable Security / Sanitization]  Not Entered |  |
| [E-# OR W-#] | Maintenance Tools [NIST 800-53 w/ DHS 4300A MA-3] | [Test: MA-3.1 - Maintenance Tools]  Not Entered | Failure to meet the requirements for maintenance tools listed below could result in loss of system integrity:  (i) the organization approves, controls, and monitors the use of information system maintenance tools; and (ii) the organization maintains information system maintenance tools on an ongoing basis. | High | [Test: MA-3.1 - Maintenance Tools]  Not Entered |  |
| [E-# OR W-#] | Response to Audit Processing Failures [NIST 800-53 w/ DHS 4300A AU-5 (2)] | [Test: AU-5(2).1 - Real-Time Alerts]  Not Entered | Failure to meet the requirements listed below for response to audit processing failures could lead to the untimely detection of an attack on or breach of the system:  (i) the organization defines audit failure events requiring real-time alerts; and, (ii) the information system provides a real-time alert when organization-defined audit failure events occur. | High | [Test: AU-5(2).1 - Real-Time Alerts]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8 (4)] | [Test: CM-8(4).1 - Accountability Information]  Not Entered | Failure ensure that the organization includes in property accountability information for information system components, a means for identifying by name, position, or role, individuals responsible for administering those components could allow difficulty in tracking personnel responsible for making faulty configurations that could affect the system functionality negatively. | High | [Test: CM-8(4).1 - Accountability Information]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (8)] | [Test: IA-2(8).1 - Network Access To Privileged Accounts - Replay Resistant]  Not Entered | Failure to meet the identification and authentication requirements listed below could result in providing any account access to critical or sensitive information:  (i) the organization defines the replay-resistant authentication mechanisms to be used for network access to privileged accounts; and (ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to privileged accounts. | High | [Test: IA-2(8).1 - Network Access To Privileged Accounts - Replay Resistant]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (4)] | [Test: CP-2(4).1 - Resume All Missions / Business Functions]  Not Entered | Failure to meet the contingency plan requirements listed below could weaken the overall security posture of the system:  (i) the organization defines the time period for planning the full resumption of affected missions and business functions as a result of contingency plan activation; and (ii) the organization plans for the full resumption of affected missions and business functions within organization-defined time period of contingency plan activation. | High | [Test: CP-2(4).1 - Resume All Missions / Business Functions]  Not Entered |  |
| [E-# OR W-#] | Media Sanitization [NIST 800-53 w/ DHS 4300A MP-6 (3)] | [Test: MP-6(3).1 - Nondestructive Techniques]  Not Entered | Failure to ensure that the organization defines circumstances requiring sanitization of portable storage devices that applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system could lead to an occurrence of unauthorized disclosure of information. | High | [Test: MP-6(3).1 - Nondestructive Techniques]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (1)] | [Test: SA-4(1).1 - Functional Properties Of Security Controls]  Not Entered | Failure of the organization to require the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed. | High | [Test: SA-4(1).1 - Functional Properties Of Security Controls]  Not Entered |  |
| [E-# OR W-#] | Security Engineering Principles [NIST 800-53 w/ DHS 4300A SA-8] | [Test: SA-8.1 - Security Engineering Principles]  Not Entered | Failure to ensure that the organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system could lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services. | High | [Test: SA-8.1 - Security Engineering Principles]  Not Entered |  |
| [E-# OR W-#] | Incident Monitoring [NIST 800-53 w/ DHS 4300A IR-5 (1)] | [Test: IR-5(1).1 - Automated Tracking / Data Collection / Analysis]  Not Entered | Failure of the organization to employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information could eventually lead to the failure to restore the system or the data causing the organization to lose assets:  (i) the organization employs automated mechanisms to assist in the tracking of security incidents; (ii) the organization employs automated mechanisms to assist in the collection of security incident information; and (iii) the organization employs automated mechanisms to assist in the analysis of security incident information. | High | [Test: IR-5(1).1 - Automated Tracking / Data Collection / Analysis]  Not Entered |  |
| [E-# OR W-#] | Supply Chain Protection [NIST 800-53 w/ DHS 4300A SA-12 (DHS-5.8.b)] | [Test: SA-12(DHS-5.8.b) - Supply Chain Threat Countermeasures]  Not Entered | Failure of the components to implement appropriate countermeasures, commensurate with the level of risk determined by the BIA to protect against the supply chain threat could result in non-secure system that lacks stability and integrity causing the unavailability of the system or the data in the system to authorized users. | High | [Test: SA-12(DHS-5.8.b) - Supply Chain Threat Countermeasures]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (4)] | [Test: AC-2(4).1 - Automated Audit Actions]  Not Entered | Failure to meet the account management requirements listed below could promote a non-standard way of handling information system account management functions resulting in inaccurate information critical to the operation of the system:  (i) the information system automatically audits:   * account creation; * modification; * disabling; and * termination actions; and   (ii) the information system notifies, as required, appropriate individuals. | High | [Test: AC-2(4).1 - Automated Audit Actions]  Not Entered |  |
| [E-# OR W-#] | Fire Protection [NIST 800-53 w/ DHS 4300A PE-13 (1)] | [Test: PE-13(1).1 - Detection Devices / Systems]  Not Entered | Failure to ensure that the organization employs fire detection devices/systems for the information system that activate automatically and notify organization-defined personnel and organization-defined emergency responders in the event of a fire could lead to accidents or personnel/employee injury due to the lack of fire detection devices/systems or due to untimely notification. | High | [Test: PE-13(1).1 - Detection Devices / Systems]  Not Entered |  |
| [E-# OR W-#] | Voice Over Internet Protocol [NIST 800-53 w/ DHS 4300A SC-19] | [Test: SC-19.1 - Voice Over Internet Protocol]  Not Entered | Failure to meet the requirements for voice over internet protocol listed below could result in information disclosure:  (i) the organization establishes usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies based on the potential to cause damage to the information system if used maliciously; and (ii) the organization authorizes, monitors, and controls the use of VoIP within the information system. | High | [Test: SC-19.1 - Voice Over Internet Protocol]  Not Entered |  |
| [E-# OR W-#] | Separation of Duties [NIST 800-53 w/ DHS 4300A AC-5] | [Test: AC-5.1 - Separation of Duties]  Not Entered | Failure to meet the requirements for separation of duties indicated below could result in the wrong assignment of rights, overlapping privileges, and overall account mismanagement:  (i) the organization separates duties of individuals as necessary, to prevent malevolent activity without collusion; (ii) the organization documents separation of duties; and (iii) the organization implements separation of duties through assigned information system access authorizations. | High | [Test: AC-5.1 - Separation of Duties]  Not Entered |  |
| [E-# OR W-#] | Media Storage [NIST 800-53 w/ DHS 4300A MP-4] | [Test: MP-4.1 - Media Storage]  Not Entered | Failure to meet the media storage requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization defines:   * types of digital and non-digital media physically controlled and securely stored within designated controlled areas; * controlled areas designated to physically control and securely store the media; * security measures to physically control and securely store the media within designated controlled areas;   (ii) the organization physically controls and securely stores organization-defined information system media within organization-defined controlled areas using organization-defined security measures; and (iii) the organization protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures. | High | [Test: MP-4.1 - Media Storage]  Not Entered |  |
| [E-# OR W-#] | Alternate Storage Site [NIST 800-53 w/ DHS 4300A CP-6] | [Test: CP-6.1 - Alternate Storage Site]  Not Entered | Failure to meet the alternate storage site requirements listed below could lead to the untimely recovery or restoration of system or of data:  (i) the organization establishes an alternate storage site; and (ii) the organization initiates necessary alternate storage site agreements to permit the storage and recovery of information system backup information. | High | [Test: CP-6.1 - Alternate Storage Site]  Not Entered |  |
| [E-# OR W-#] | Developer-Provided Training [NIST 800-53 w/ DHS 4300A SA-16] | [Test: SA-16.1 - Developer-Provided Training]  Not Entered | Failure to ensure that the organization requires the developer of the information system, system component, or information system service to provide organization-defined training on the correct use and operation of the implemented security functions, controls, and/or mechanisms could result in the inability to respond properly to an incident, leading to the disruption of critical mission/business functions, operations, and processes. | High | [Test: SA-16.1 - Developer-Provided Training]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8 (3)] | [Test: CM-8(3).1 - Automated Unauthorized Component Detection]  Not Entered | Failure to meet the information system component inventory requirements listed below could eventually lead to the loss of critical resources due to the absence of tracking process that could detect missing critical components in a timely fashion:  (i) the organization defines the frequency of employing automated mechanisms to detect the addition of unauthorized components/devices into the information system; (ii) the organization employs automated mechanisms, in accordance with the organization-defined frequency, to detect the addition of unauthorized components/devices into the information system; and (iii) the organization disables network access by such components/devices or notifies designated organizational officials. | High | [Test: CM-8(3).1 - Automated Unauthorized Component Detection]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (2)] | [Test: AC-6(2).1 - Non-Privileged Access For Nonsecurity Functions]  Not Entered | Failure to meet the least privilege requirements listed below could leave the system vulnerable to unauthorized access:  (i) the organization defines the security functions or security-relevant information to which users of information system accounts, or roles, have access; (ii) the organization requires that users of information system accounts, or roles, with access to organization-defined security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions; and, (iii) the organization, if deemed feasible, audits any use of privileged accounts, or roles, with access to organization-defined security functions or security-relevant information, when accessing other system functions. | High | [Test: AC-6(2).1 - Non-Privileged Access For Nonsecurity Functions]  Not Entered |  |
| [E-# OR W-#] | Access Restrictions for Change [NIST 800-53 w/ DHS 4300A CM-5 (1)] | [Test: CM-5(1).1 - Automated Access Enforcement / Auditing]  Not Entered | Failure of the organization to employ automated mechanisms to enforce access restrictions and support auditing of the enforcement actions could allow any user to effect system wide modification without being detected in a timely manner and cause the system to be unstable or lose its integrity. | High | [Test: CM-5(1).1 - Automated Access Enforcement / Auditing]  Not Entered |  |
| [E-# OR W-#] | Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7 (2)] | [Test: CP-7(2).1 - Accessibility]  Not Entered | Failure to meet the requirements for alternate processing site indicated below could result in the system or data being unavailable when needed or, possibly, could lead to the discontinuation of the entire business operations/processes:  (i) the organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster; and (ii) the organization outlines explicit mitigation actions for organization identified accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster. | High | [Test: CP-7(2).1 - Accessibility]  Not Entered |  |
| [E-# OR W-#] | Water Damage Protection [NIST 800-53 w/ DHS 4300A PE-15 (1)] | [Test: PE-15(1).1 - Automation Support]  Not Entered | Failure of the organization to employ automated mechanisms to detect the presence of water in the vicinity of the information system and alerts organization-defined personnel could endanger the facilities, systems, data/information, and personnel/employees. | High | [Test: PE-15(1).1 - Automation Support]  Not Entered |  |
| [E-# OR W-#] | Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7 (3)] | [Test: CP-7(3).1 - Priority Of Service]  Not Entered | Failure to ensure that the organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements could result in the system or data being unavailable when needed; or, could possibly lead to the discontinuation of the entire business operations/processes. | High | [Test: CP-7(3).1 - Priority Of Service]  Not Entered |  |
| [E-# OR W-#] | Time Stamps [NIST 800-53 w/ DHS 4300A AU-8 (1)] | [Test: AU-8(1).1 - Synchronization With Authoritative Time Source]  Not Entered | Failure to meet the time stamp requirements listed below could result in the untimely tracking or detection of attack on the system, which could lead to the complete compromise of the system or of the data in the system:  (i) the organization defines the frequency of internal clock synchronization for the information system; (ii) the organization defines the authoritative time source for internal clock synchronization; and (iii) the organization synchronizes internal information system clocks with the organization-defined authoritative time source in accordance with the organization-defined frequency. | High | [Test: AU-8(1).1 - Synchronization With Authoritative Time Source]  Not Entered |  |
| [E-# OR W-#] | Access Restrictions for Change [NIST 800-53 w/ DHS 4300A CM-5 (3)] | [Test: CM-5(3).1 - Signed Components]  Not Entered | Failure to meet the access restrictions for change requirements listed below could allow any user to effect system wide modification without being detected in a timely manner and cause the system to be unstable or lose its integrity:  (i) the organization defines critical software programs that the information system will prevent from being installed if such software programs are not signed with a recognized and approved certificate; and (ii) the information system prevents the installation of organization-defined critical software programs that are not signed with a certificate that is recognized and approved by the organization. | High | [Test: CM-5(3).1 - Signed Components]  Not Entered |  |
| [E-# OR W-#] | Prohibit Use Without Owner [NIST 800-53 w/ DHS 4300A MP-7 (1)] | [Test: MP-7(1).1 - Prohibit Use Without Owner]  Not Entered | Failure to ensure that the organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner could leave the system vulnerable to data extraction or corruption depending on the mode of attack used. | High | [Test: MP-7(1).1 - Prohibit Use Without Owner]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (2)] | [Test: CP-2(2).1 - Capacity Planning]  Not Entered | Failure to ensure that the organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations could prevent a possible overload of security rules and redundancy of policies that will be placed in effect. | High | [Test: CP-2(2).1 - Capacity Planning]  Not Entered |  |
| [E-# OR W-#] | Development Process, Standards, and Tools [NIST 800-53 w/ DHS 4300A SA-15] | [Test: SA-15.1 - Development Process, Standards, and Tools]  Not Entered | Failure to meet the development process, standards, and tools requirements indicated below could result in the acquisition of inherently unsafe/non-secure systems that would expose the organization to other exploits and threats/vulnerabilities, which could eventually lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services:  (i) the organization requires the developer of the information system, system component, or information system service to follow a documented development process that:   * explicitly addresses security requirements; * identifies the standards and tools used in the development process; * Documents the specific tool options and tool configurations used in the development process; and * Documents, manages, and ensures the integrity of changes to the process and/or tools used in development; and   (ii) the organization reviews the development process, standards, tools, and tool options/configurations organization-defined frequency to determine if the process, standards, tools, and tool options/configurations selected and employed can satisfy organization defined security requirements. | High | [Test: SA-15.1 - Development Process, Standards, and Tools]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6] | [Test: AC-6.1 - Least Privilege]  Not Entered | Failure to ensure that the organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions could result in the non-completion of critical and required tasks by users of the information system. | High | [Test: AC-6.1 - Least Privilege]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (3)] | [Test: IA-2(3).1 - Local Access To Privileged Accounts]  Not Entered | Failure to ensure that the information system uses multifactor authentication for local access to privileged accounts could result in providing any account access to critical or sensitive information. | High | [Test: IA-2(3).1 - Local Access To Privileged Accounts]  Not Entered |  |
| [E-# OR W-#] | User-Based Collaboration and Information Sharing [NIST 800-53 w/ DHS 4300A AC-21] | [Test: AC-21.1 - Information Sharing]  Not Entered | Failure to meet the user-based collaboration and information sharing requirements listed below could leave essential data exposed to unauthorized access and viewing by individuals not connected to the organization:  (i) the organization defines the circumstances where user discretion is required to facilitate information sharing; (ii) the organization facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information for the organization-defined circumstances; (iii) the organization defines the information sharing circumstances and automated mechanisms or manual processes required to assist users in making information sharing/collaboration decisions; and, (iv) the organization employs organization-defined circumstances and automated mechanisms or manual processes to assist users in making information sharing/collaboration decisions. | High | [Test: AC-21.1 - Information Sharing]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (DHS-5.1.1.e)] | [Test: SI-7(DHS-5.1.1.e) - Embedded Passwords]  Not Entered | Failure of the components to prohibit passwords from being embedded in scripts or source code could eventually lead to disclosure or compromise of high-level information. | High | [Test: SI-7(DHS-5.1.1.e) - Embedded Passwords]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (5)] | [Test: AC-2(5).1 - Inactivity Logout]  Not Entered | Failure to require users to log out in accordance with the organization-defined time-period of inactivity and/or description of when to log out could leave the system vulnerable to improper utilization of resources due to unmonitored usage times of systems and non-compliance to access restrictions that are critical to the overall durability of organizational assets. | High | [Test: AC-2(5).1 - Inactivity Logout]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7] | [Test: SI-7.1 - Software, Firmware, and Information Integrity]  Not Entered | Failure to ensure that the organization employs integrity verification tools to detect unauthorized changes to organization-defined software, firmware, and information could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-7.1 - Software, Firmware, and Information Integrity]  Not Entered |  |
| [E-# OR W-#] | Media Transport [NIST 800-53 w/ DHS 4300A MP-5] | [Test: MP-5.1 - Media Transport]  Not Entered | Failure to meet the media transport requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization protects and controls organization-defined types of digital and non-digital media during transport outside of controlled areas using organization-defined security safeguards; (ii) the organization maintains accountability for information system media during transport outside of controlled areas; and, (iii) the organization restricts the activities associated with transport of such media to authorized personnel. | High | [Test: MP-5.1 - Media Transport]  Not Entered |  |
| [E-# OR W-#] | Incident Response Assistance [NIST 800-53 w/ DHS 4300A IR-7 (1)] | [Test: IR-7(1).1 - Automation Support For Availability Of Information / Support]  Not Entered | Failure of the organization to employ automated mechanisms to increase the availability of incident response-related information and support for incident response support could result in the lack of awareness regarding the ways to respond to incidents, eventually leading to the loss of critical mission/business assets. | High | [Test: IR-7(1).1 - Automation Support For Availability Of Information / Support]  Not Entered |  |
| [E-# OR W-#] | Response to Audit Processing Failures [NIST 800-53 w/ DHS 4300A AU-5 (1)] | [Test: AU-5(1).1 - Audit Storage Capacity]  Not Entered | Failure to meet the requirements listed below for response to audit processing failures could result in the failure of disaster avoidance where data critical to an accurate audit report could be damaged without personnel responsible for its maintenance being alerted:   (i) the organization defines the percentage of maximum audit record storage capacity that, if reached, requires a warning to be provided; and, (ii) the information system provides a warning when the allocated audit record storage volume reaches the organization-defined percentage of maximum audit record storage capacity. | High | [Test: AU-5(1).1 - Audit Storage Capacity]  Not Entered |  |
| [E-# OR W-#] | Alternate Storage Site [NIST 800-53 w/ DHS 4300A CP-6 (2)] | [Test: CP-6(2).1 - Recovery Time / Point Objectives]  Not Entered | Failure to ensure that the alternate storage site is configured to enable timely and effective recovery operations could lead to the untimely recovery or restoration of system or of data. | High | [Test: CP-6(2).1 - Recovery Time / Point Objectives]  Not Entered |  |
| [E-# OR W-#] | Information System Backup [NIST 800-53 w/ DHS 4300A CP-9 (2)] | [Test: CP-9(2).1 - Test Restoration Using Sampling]  Not Entered | Failure of the organization to use selected backup information in the restoration of information system functions as part of contingency plan testing could result in the loss of data or of system integrity due to ineffective or untested backup process/reliability, which could lead to the disruption of critical mission/business functions, operations, and processes. | High | [Test: CP-9(2).1 - Test Restoration Using Sampling]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (2)] | [Test: CM-6(2).1 - Respond To Unauthorized Changes]  Not Entered | Failure to meet the configuration settings requirements listed below could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or technology products:  (i) the organization defines configuration settings that, if modified by unauthorized changes, initiate the automated mechanisms to be employed to respond to such changes; and (ii) the organization employs automated mechanisms to respond to unauthorized changes to organization-defined configuration settings. | High | [Test: CM-6(2).1 - Respond To Unauthorized Changes]  Not Entered |  |
| [E-# OR W-#] | Supply Chain Protection [NIST 800-53 w/ DHS 4300A SA-12] | [Test: SA-12.1 - Supply Chain Protection]  Not Entered | Failure to meet the supply chain protection requirements indicated below could leave the system more exposed to vulnerabilities:  (i) the organization defines the measures to be employed to protect against supply chain threats; and (ii) the organization protects against supply chain threats by employing organization-defined measures as part of a comprehensive, defense-in-breadth information security strategy. | High | [Test: SA-12.1 - Supply Chain Protection]  Not Entered |  |
| [E-# OR W-#] | Configuration Change Control [NIST 800-53 w/ DHS 4300A CM-3 (DHS-5.4.3.l)] | [Test: CM-3(DHS-5.4.3.l) - DHS Change Control Boards(CCB)]  Not Entered | Failure to meet the configuration change control requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the Control Change Board (CCB) determines the types of changes to the information system that are configuration controlled; and  (ii) the CCB documents approved configuration-controlled changes to the system, including DHS systems that interface with OneNet. | High | [Test: CM-3(DHS-5.4.3.l) - DHS Change Control Boards(CCB)]  Not Entered |  |
| [E-# OR W-#] | Malicious Code Protection [NIST 800-53 w/ DHS 4300A SI-3 (2)] | [Test: SI-3(2).1 - Automatic Updates]  Not Entered | Failure of the organization to automatically update malicious code protection mechanisms could result in the inability to detect in a timely fashion any threats/vulnerabilities and exploits identified with and inherent in malicious codes enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-3(2).1 - Automatic Updates]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan Testing and Exercises [NIST 800-53 w/ DHS 4300A CP-4 (1)] | [Test: CP-4(1).1 - Coordinate With Related Plans]  Not Entered | Failure of the organization to coordinate contingency plan testing and/or exercises with organizational elements responsible for related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan) could result in the inability to restore the overall, business-related system or data in a timely manner due to ineffective and untested contingency plan, which could lead to the unavailability of critical resources or data. | High | [Test: CP-4(1).1 - Coordinate With Related Plans]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (2)] | [Test: IA-2(2).1 - Network Access To Non-Privileged Accounts]  Not Entered | Failure to ensure that the information system uses multifactor authentication for network access to non-privileged accounts could result in the absence of personnel responsibility and accountability or in ineffective identification and authentication policy, which could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data. | High | [Test: IA-2(2).1 - Network Access To Non-Privileged Accounts]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (11)] | [Test: AC-2(11).1 - Usage Conditions]  Not Entered | Failure to describe the specific conditions or circumstances under which information system accounts can be used could leave the system vulnerable to improper utilization of resources due to unmonitored activity of access. | High | [Test: AC-2(11).1 - Usage Conditions]  Not Entered |  |
| [E-# OR W-#] | Device Identification and Authentication [NIST 800-53 w/ DHS 4300A IA-3] | [Test: IA-3.1 - Device Identification and Authentication]  Not Entered | Failure to meet the user identification and authentication requirements listed below could lead to any attacker or malicious user gaining unauthorized access to or elevated privileges on the system or the data through specific devices that the information system could not properly identify/authorize:  (i) the organization defines the specific and/or types of devices for which identification and authentication is required before establishing a connection to the information system; and (ii) the information system uniquely identifies and authenticates the organization-defined devices before establishing a connection to the information system. | High | [Test: IA-3.1 - Device Identification and Authentication]  Not Entered |  |
| [E-# OR W-#] | Fail in Known State [NIST 800-53 w/ DHS 4300A SC-24] | [Test: SC-24.1 - Fail in Known State]  Not Entered | Failure to ensure that the information system fails to a organization-defined known-state for organization-defined types of failures preserving organization-defined system state information in failure could leave the system vulnerable to several other critical security concerns resulting from non-compliance of known standards and rules. | High | [Test: SC-24.1 - Fail in Known State]  Not Entered |  |
| [E-# OR W-#] | Access Control for Mobile Devices [NIST 800-53 w/ DHS 4300A AC-19 (5)] | [Test: AC-19(5).1 - Full Device / Container-Based Encryption]  Not Entered | Failure to employ container-based encryption to protect the confidentiality and integrity of information on mobile devices could lead to an occurrence of unauthorized disclosure of information. | High | [Test: AC-19(5).1 - Full Device / Container-Based Encryption]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7 (1)] | [Test: CM-7(1).1 - Periodic Review]  Not Entered | Failure to meet the least functionality requirements listed below could allow any user to perform other functions without restrictions or, possibly, could allow any attacker to gain unauthorized access to the system or the data in the system:  (i) the organization defines the frequency of information system reviews to identify and eliminate unnecessary:   * functions; * ports; * protocols; and/or * services; and   (ii) the organization reviews the information system in accordance with organization- defined frequency to identify and eliminate unnecessary:   * functions; * ports; * protocols; and/or * services. | High | [Test: CM-7(1).1 - Periodic Review]  Not Entered |  |
| [E-# OR W-#] | Security Assessments [NIST 800-53 w/ DHS 4300A CA-2 (1)] | [Test: CA-2(1).1 - Independent Assessors]  Not Entered | Failure to ensure that the organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system could allow certain security holes to exist not discovered by internal assessment teams. | High | [Test: CA-2(1).1 - Independent Assessors]  Not Entered |  |
| [E-# OR W-#] | Wireless Access [NIST 800-53 w/ DHS 4300A AC-18 (1)] | [Test: AC-18(1).1 - Authentication And Encryption]  Not Entered | Failure of the organization to use authentication and encryption to protect wireless access to the information system could result in information disclosure by trying to intercept a session that terminates to the system if the organization uses authentication and encryption to protect wireless access to the information system. | High | [Test: AC-18(1).1 - Authentication And Encryption]  Not Entered |  |
| [E-# OR W-#] | Security Function Isolation [NIST 800-53 w/ DHS 4300A SC-3] | [Test: SC-3.1 - Security Function Isolation]  Not Entered | Failure to ensure that the information system isolates security functions from nonsecurity functions could try to exploit using various vectors and compromise the system or the data in the system | High | [Test: SC-3.1 - Security Function Isolation]  Not Entered |  |
| [E-# OR W-#] | Emergency Shutoff [NIST 800-53 w/ DHS 4300A PE-10] | [Test: PE-10.1 - Emergency Shutoff]  Not Entered | Failure to meet the requirements for emergency shutoff listed below could lead to the compromise of the system or of the data in the system:  (i) the organization provides the capability of shutting off power to the information system or individual system components in emergency situations; (ii) the organization places emergency shutoff switches or devices in organization-defined location by information system or system component to facilitate safe and easy access for personnel; and, (iii) the organization protects emergency power shutoff capability from unauthorized activation.e emergency power shutoff capability from unauthorized activation. | High | [Test: PE-10.1 - Emergency Shutoff]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (14)] | [Test: SI-7(14).1 - Binary Or Machine Executable Code]  Not Entered | Failure to meet the requirements for binary or machine executable code listed below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization prohibits the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code; and (ii) the organization provides exceptions to the source code requirement only for compelling mission/operational requirements and with the approval of the authorizing official. | High | [Test: SI-7(14).1 - Binary Or Machine Executable Code]  Not Entered |  |
| [E-# OR W-#] | Monitoring Physical Access [NIST 800-53 w/ DHS 4300A PE-6 (1)] | [Test: PE-6(1).1 - Intrusion Alarms / Surveillance Equipment]  Not Entered | Failure to ensure that the organization monitors physical intrusion alarms and surveillance equipment could lead to the compromise of the system or to the disclosure of information. | High | [Test: PE-6(1).1 - Intrusion Alarms / Surveillance Equipment]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (4)] | [Test: IA-2(4).1 - Local Access To Non-Privileged Accounts]  Not Entered | Failure to ensure that the information system uses multifactor authentication for local access to non-privileged accounts could result in providing any account access to critical or sensitive information. | High | [Test: IA-2(4).1 - Local Access To Non-Privileged Accounts]  Not Entered |  |
| [E-# OR W-#] | Information Flow Enforcement [NIST 800-53 w/ DHS 4300A AC-4] | [Test: AC-4.1 - Information Flow Enforcement]  Not Entered | Failure of the information system to use protected processing domains could result in an unsuitable, inaccurate or unreliable information flow enforcement control implementation. | High | [Test: AC-4.1 - Information Flow Enforcement]  Not Entered |  |
| [E-# OR W-#] | Session Lock [NIST 800-53 w/ DHS 4300A AC-11 (1)] | [Test: AC-11(1).1 - Pattern-Hiding Displays]  Not Entered | Failure to ensure that the information system session conceals information previously visible on the display with a publicly viewable image could leave essential data visible to non-authorized personnel. | High | [Test: AC-11(1).1 - Pattern-Hiding Displays]  Not Entered |  |
| [E-# OR W-#] | Mobile Code [NIST 800-53 w/ DHS 4300A SC-18] | [Test: SC-18.1 - Mobile Code]  Not Entered | Failure to meet the mobile code requirements indicated below could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system:  (i) the organization defines acceptable and unacceptable mobile code and mobile code technologies; (ii) the organization establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and (iii) the organization authorizes, monitors, and controls the use of mobile code within the information system. | High | [Test: SC-18.1 - Mobile Code]  Not Entered |  |
| [E-# OR W-#] | Transmission Integrity [NIST 800-53 w/ DHS 4300A SC-8] | [Test: SC-8.1 - Transmission Confidentiality and Integrity]  Not Entered | Failure of the information system to protect the confidentiality or integrity of transmitted information could leave the system more exposed to vulnerabilities, which an attacker could try to exploit using various vectors and compromise the system or the data in the system. | High | [Test: SC-8.1 - Transmission Confidentiality and Integrity]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5 (2)] | [Test: IA-5(2).1 - PKI-Based Authentication]  Not Entered | Failure to ensure that the information system, for PKI-based authentication correspond to the following could leave the system vulnerable to unauthorized access, impersonation, and brute force attacks:   * validates certificates by constructing a certification path with status information to an accepted trust anchor; * enforces authorized access to the corresponding private key; and * maps the authenticated identity to the user account. | High | [Test: IA-5(2).1 - PKI-Based Authentication]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (6)] | [Test: AU-6(6).1 - Correlation With Physical Monitoring]  Not Entered | Failure to ensure that the organization correlates information from audit records with information obtained from monitoring physical access to enhance the ability to identify suspicious, inappropriate, unusual, or malevolent activity could prevent the proper implementation of standard audit requirements and protocols. | High | [Test: AU-6(6).1 - Correlation With Physical Monitoring]  Not Entered |  |
| [E-# OR W-#] | Telecommunications Services [NIST 800-53 w/ DHS 4300A CP-8 (2)] | [Test: CP-8(2).1 - Single Points Of Failure]  Not Entered | Failure of the organization to obtain alternate telecommunications services that do not share a single point of failure with primary telecommunications services could leave the system unavailable or inaccessible when either the primary or the alternate telecommunications service is down. | High | [Test: CP-8(2).1 - Single Points Of Failure]  Not Entered |  |
| [E-# OR W-#] | Information System Monitoring [NIST 800-53 w/ DHS 4300A SI-4 (4)] | [Test: SI-4(4).1 - Inbound And Outbound Communications Traffic]  Not Entered | Failure to ensure that the information system monitors inbound and outbound communications traffic organization-defined frequency for unusual or unauthorized activities or conditions could result in the inability to detect any attack on, intrusion of or unusual/unauthorized use of the information system enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-4(4).1 - Inbound And Outbound Communications Traffic]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (5)] | [Test: AC-6(5).1 - Privileged Accounts]  Not Entered | Failure to ensure that the organization limits authorization to super user accounts on the information system to designated system administration personnel could compromise the overall stability of the system should unqualified personnel be allowed access to essential system controls and configuration tools. | High | [Test: AC-6(5).1 - Privileged Accounts]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (3)] | [Test: AC-6(3).1 - Network Access To Privileged Commands]  Not Entered | Failure to meet the least privilege requirements listed below could leave the system vulnerable to impersonation attacks leading to compromise of system related controls or extraction of essential data:  (i) the organization defines the privileged commands to which network access is to be authorized only for compelling operational needs; (ii) the organization authorizes network access to organization-defined privileged commands only for compelling operational needs; and (iii) the organization documents the rationale for authorized network access to organization-defined privileged commands in the security plan for the information system. | High | [Test: AC-6(3).1 - Network Access To Privileged Commands]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (5)] | [Test: AU-6(5).1 - Integration / Scanning And Monitoring Capabilities]  Not Entered | Failure to ensure that the organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to enhance the ability to identify inappropriate or unusual activity could prevent the proper implementation of standard audit requirements and protocols. | High | [Test: AU-6(5).1 - Integration / Scanning And Monitoring Capabilities]  Not Entered |  |
| [E-# OR W-#] | Media Sanitization [NIST 800-53 w/ DHS 4300A MP-6 (1)] | [Test: MP-6(1).1 - Review / Approve / Track / Document / Verify]  Not Entered | Failure of the organization to review, approve, track, document, and verify media sanitization and disposal actions could result in the inability to detect the disclosure of critical and sensitive mission/business information due to the inappropriate or unapproved of disposal process. | High | [Test: MP-6(1).1 - Review / Approve / Track / Document / Verify]  Not Entered |  |
| [E-# OR W-#] | Protection of Audit Information [NIST 800-53 w/ DHS 4300A AU-9 (2)] | [Test: AU-9(2).1 - Audit Backup On Separate Physical Systems / Components]  Not Entered | Failure to meet the protection of audit information requirements listed below could result in the loss of integrity of the audit information or of the audit tools, which could invalidate any result of forensic investigation:  (i) the organization defines the system or media for storing back up audit records that is a different system or media than the system being audited; (ii) the organization defines the frequency of information system backups of audit records; and, (iii) the information system backs up audit records, in accordance with the organization- defined frequency, onto organization-defined system or media. | High | [Test: AU-9(2).1 - Audit Backup On Separate Physical Systems / Components]  Not Entered |  |
| [E-# OR W-#] | Application Partitioning [NIST 800-53 w/ DHS 4300A SC-2] | [Test: SC-2.1 - Application Partitioning]  Not Entered | Failure of the information system to separate user functionality (including user interface services) from information system management functionality could lead to the instability of the system. | High | [Test: SC-2.1 - Application Partitioning]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5 (5)] | [Test: RA-5(5).1 - Privileged Access]  Not Entered | Failure to meet the vulnerability scanning requirement listed below could result in unauthorized disclosure of information, greater compromise of the system, or to other more severe security threats against the organization:  (i) the organization includes privileged access authorization to organization-defined information system components identified for selected vulnerability scanning activities to facilitate more thorough scanning; and, (ii) the organization defines the list of information system components to which privileged access is authorized for selected vulnerability scanning activities. | High | [Test: RA-5(5).1 - Privileged Access]  Not Entered |  |
| [E-# OR W-#] | Incident Response Training [NIST 800-53 w/ DHS 4300A IR-2 (1)] | [Test: IR-2(1).1 - Simulated Events]  Not Entered | Failure of the organization to incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations could result in the inability to respond properly to an incident, leading to the disruption of critical mission/business functions, operations, and processes. | High | [Test: IR-2(1).1 - Simulated Events]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5 (1)] | [Test: RA-5(1).1 - Update Tool Capability]  Not Entered | Failure to ensure that the organization employs vulnerability scanning tools that have the capability to readily update the list of information system vulnerabilities scanned could lead to exploitation by attackers when users visit infected web sites. | High | [Test: RA-5(1).1 - Update Tool Capability]  Not Entered |  |
| [E-# OR W-#] | Public Key Infrastructure Certificates [NIST 800-53 w/ DHS 4300A SC-17] | [Test: SC-17.1 - Public Key Infrastructure Certificates]  Not Entered | Failure to meet the organization issues public key certificates under an organization-defined certificate policy or obtains public key certificates from an approved service provider could result in the compromise of the system or of the data in the system. | High | [Test: SC-17.1 - Public Key Infrastructure Certificates]  Not Entered |  |
| [E-# OR W-#] | Information Input Validation [NIST 800-53 w/ DHS 4300A SI-10] | [Test: SI-10.1 - Information Input Validation]  Not Entered | Failure to ensure that the information system checks the validity of information inputs could result in the loss of information system integrity and stability, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-10.1 - Information Input Validation]  Not Entered |  |
| [E-# OR W-#] | Cryptographic Key Establishment and Management [NIST 800-53 w/ DHS 4300A SC-12 (1)] | [Test: SC-12(1).1 - Availability]  Not Entered | Failure to ensure that the organization maintains availability of information in the event of the loss of cryptographic keys by users could lead to the disclosure of critical mission/business information/data. | High | [Test: SC-12(1).1 - Availability]  Not Entered |  |
| [E-# OR W-#] | Supply Chain Protection [NIST 800-53 w/ DHS 4300A SA-12 (DHS-5.8.a)] | [Test: SA-12(DHS-5.8.a) - Business Impact Assessments(BIA)]  Not Entered | Failure to ensure that the Business Impact Assessments (BIA) are used to determine the level of risk introduced to the system by the IT supply chain and whether the IT supply chain threat introduces sufficient risk to require the implementation of countermeasures could lead to disclosure of confidentiality, integrity, and availability standard as specified by the organization's policy. | High | [Test: SA-12(DHS-5.8.a) - Business Impact Assessments(BIA)]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (DHS-3.9.b)] | [Test: CM-2(DHS-3.9.b) - FIPS 199 and FIPS 200 Usage]  Not Entered | Failure to employ NIST-based security controls could make it difficult for the organization to determine appropriate levels of protection for information all systems. | High | [Test: CM-2(DHS-3.9.b) - FIPS 199 and FIPS 200 Usage]  Not Entered |  |
| [E-# OR W-#] | Developer Security Architecture and Design [NIST 800-53 w/ DHS 4300A SA-17] | [Test: SA-17.1 - Developer Security Architecture and Design]  Not Entered | Failure to ensure that the organization requires the developer of the information system, system component, or information system service to produce a design specification and security architecture that indicated below could lead to instability of the system or possibly to the compromise of the system:  (i) Is consistent with and supportive of the security architecture established within the enterprise architecture;  (ii) Accurately and completely describes the required security functionality, and the allocation of security controls among physical and logical components; and  (iii) Expresses how individual security functions, mechanisms, and services work together to provide required security capabilities and a unified approach to protection. | High | [Test: SA-17.1 - Developer Security Architecture and Design]  Not Entered |  |
| [E-# OR W-#] | Error Handling [NIST 800-53 w/ DHS 4300A SI-11] | [Test: SI-11.1 - Error Handling]  Not Entered | Failure to meet the requirements for error handling listed below could lead to the instability of the system:  (i) the organization generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and (ii) the organization reveals error messages only to organization-defined personnel or roles. | High | [Test: SI-11.1 - Error Handling]  Not Entered |  |
| [E-# OR W-#] | Maintenance Personnel [NIST 800-53 w/ DHS 4300A MA-5 (1)] | [Test: MA-5(1).1 - Individuals Without Appropriate Access]  Not Entered | Failure to ensure that the organization maintains procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that are listed below could lead to the compromise of system confidentiality and disclosure of classified information:   * maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the information system by approved organizational personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; * prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances, or formal access approvals, all volatile   information storage components within the information system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and   * in the event an information system component cannot be sanitized, the procedures contained in the security plan for the system are enforced. | High | [Test: MA-5(1).1 - Individuals Without Appropriate Access]  Not Entered |  |
| [E-# OR W-#] | Continuous Monitoring [NIST 800-53 w/ DHS 4300A CA-7 (1)] | [Test: CA-7(1).1 - Independent Assessment]  Not Entered | Failure of the organization to employ an independent certification agent or certification team to monitor the security controls in the information system on an ongoing basis could render the security controls useless if there would be bias in the monitoring of the in-house agent or team. | High | [Test: CA-7(1).1 - Independent Assessment]  Not Entered |  |
| [E-# OR W-#] | Content of Audit Records [NIST 800-53 w/ DHS 4300A AU-3 (2)] | [Test: AU-3(2).1 - Centralized Management Of Planned Audit Record Content]  Not Entered | Failure of the information system to provide the capability to centrally manage the content of audit records generated from multiple components throughout the system could lead to the untimely detection of any attack on the system:  (i) the organization defines the information system components for which the content of audit records generated is centrally managed; and, (ii) the organization centrally manages the content of audit records generated by organization-defined information system components. | High | [Test: AU-3(2).1 - Centralized Management Of Planned Audit Record Content]  Not Entered |  |
| [E-# OR W-#] | Telecommunications Services [NIST 800-53 w/ DHS 4300A CP-8 (1)] | [Test: CP-8(1).1 - Priority Of Service Provisions]  Not Entered | Failure of the organization to develop primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements could leave the system or the data unavailable when needed by clients or users:  (i) the organization develops primary and alternate telecommunications service agreements that contain priority-of-service provisions in accordance with organizational availability requirements; and (ii) the organization requests Telecommunications Service Priority for all telecommunications services used for national security emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier. | High | [Test: CP-8(1).1 - Priority Of Service Provisions]  Not Entered |  |
| [E-# OR W-#] | Spam Protection [NIST 800-53 w/ DHS 4300A SI-8] | [Test: SI-8.1 - Spam Protection]  Not Entered | Failure of the information system to implement spam protection by following the requirements listed below could lead to information disclosure:  (i) the organization mploys spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages; and (ii) the organization updates spam protection mechanisms when new releases are available in accordance with organizational configuration management policy and procedures. | High | [Test: SI-8.1 - Spam Protection]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (2)] | [Test: SI-7(2).1 - Automated Notifications Of Integrity Violations]  Not Entered | Failure to ensure that the organization employs automated tools that provide notification to organization-defined personnel or roles upon discovering discrepancies during integrity verification could result in the untimely remediation of discrepancies on/of information system functionality, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-7(2).1 - Automated Notifications Of Integrity Violations]  Not Entered |  |
| [E-# OR W-#] | Maintenance Tools [NIST 800-53 w/ DHS 4300A MA-3 (3)] | [Test: MA-3(3).1 - Prevent Unauthorized Removal]  Not Entered | Failure of the organization to either (a) check all maintenance equipment with the capability of retaining information so that no organizational information is written on the equipment or the equipment is appropriately sanitized before release; or (b) retain the maintenance equipment within the facility or destroys the equipment if the equipment cannot be sanitized, unless an appropriate organization official explicitly authorizes an exception, could lead to the system losing its integrity or its stability and possibly to the disclosure of critical and sensitive information. | High | [Test: MA-3(3).1 - Prevent Unauthorized Removal]  Not Entered |  |
| [E-# OR W-#] | Incident Response Testing and Exercises [NIST 800-53 w/ DHS 4300A IR-3] | [Test: IR-3.1 - Incident Response Testing]  Not Entered | Failure to meet the incident response testing and exercises requirements listed below could result in the inability to respond properly to an incident and in a timely manner, which could lead to the disruption of critical mission/business functions, operations, and processes:  (i) the organization defines incident response tests/exercises; (ii) the organization defines the frequency of incident response tests/exercises; (iii) the organization tests/exercises the incident response capability for the information system using organization-defined tests/exercises in accordance with organization- defined frequency; (iv) the organization documents the results of incident response tests/exercises; and (v) the organization determines the effectiveness of the incident response capability. | High | [Test: IR-3.1 - Incident Response Testing]  Not Entered |  |
| [E-# OR W-#] | Location of Information System Components [NIST 800-53 w/ DHS 4300A PE-18] | [Test: PE-18.1 - Location of Information System Components]  Not Entered | Failure to ensure that the organization positions information system components within the facility to minimize potential damage from organization-defined physical and environmental hazards and to minimize the opportunity for unauthorized access could lead to exposure of the system to potential damage from physical/environmental hazards and to unauthorized access. | High | [Test: PE-18.1 - Location of Information System Components]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (2)] | [Test: AC-17(2).1 - Protection Of Confidentiality / Integrity Using Encryption]  Not Entered | Failure of the information system to employ cryptography to protect the confidentiality and integrity of remote access sessions could result in the disclosure of critical or sensitive information. | High | [Test: AC-17(2).1 - Protection Of Confidentiality / Integrity Using Encryption]  Not Entered |  |
| [E-# OR W-#] | Emergency Power [NIST 800-53 w/ DHS 4300A PE-11 (1)] | [Test: PE-11(1).1 - Long-Term Alternate Power Supply - Minimal Operational Capability]  Not Entered | Failure of the organization to provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source could result in the unavailability of critical mission/business information on systems. | High | [Test: PE-11(1).1 - Long-Term Alternate Power Supply - Minimal Operational Capability]  Not Entered |  |
| [E-# OR W-#] | Audit Reduction and Report Generation [NIST 800-53 w/ DHS 4300A AU-7] | [Test: AU-7.1 - Audit Reduction and Report Generation]  Not Entered | Failure of the information system to provide audit reduction and report generation tools that support after-the-fact investigations of security incidents without altering original audit records could result in unwanted amount of information, which could lead to the inability to track in a timely manner any attack on the system or data. | High | [Test: AU-7.1 - Audit Reduction and Report Generation]  Not Entered |  |
| [E-# OR W-#] | Media Marking [NIST 800-53 w/ DHS 4300A MP-3] | [Test: MP-3.1 - Media Marking]  Not Entered | Failure to meet the media marking requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization marks removable media and information system output in accordance with organizational policies and procedures, indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and, (ii) the organization defines removable media types output exempt from marking as long as the exempted items remain within controlled areas designated. | High | [Test: MP-3.1 - Media Marking]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (4)] | [Test: AC-17(4).1 - Privileged Commands / Access]  Not Entered | Failure to meet the remote access requirements listed below could result in the non-completion of critical tasks by users requiring remote access to resources in the information system:  (i) the organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs; and (ii) the organization documents the rationale for such access in the security plan for the information system. | High | [Test: AC-17(4).1 - Privileged Commands / Access]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (3)] | [Test: CM-2(3).1 - Retention Of Previous Configurations]  Not Entered | Failure to ensure that the organization retains older versions of baseline configurations as deemed necessary to support rollback could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or of systems that need configuration updates. | High | [Test: CM-2(3).1 - Retention Of Previous Configurations]  Not Entered |  |
| [E-# OR W-#] | Information System Recovery and Reconstitution [NIST 800-53 w/ DHS 4300A CP-10 (4)] | [Test: CP-10(4).1 - Restore Within Time Period]  Not Entered | Failure to meet the information system recovery and reconstitution requirements listed below could result in the loss of system integrity or stability, which could lead to the disruption of critical mission/business functions, operations, and processes:  (i) the organization defines the time-periods within which information system components must be re-imaged from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components; and (ii) the organization provides the capability to re-image information system components, within organization-defined time-periods, from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components. | High | [Test: CP-10(4).1 - Restore Within Time Period]  Not Entered |  |
| [E-# OR W-#] | Use of External Information Systems [NIST 800-53 w/ DHS 4300A AC-20 (2)] | [Test: AC-20(2).1 - Portable Storage Devices]  Not Entered | Failure to ensure that the organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems could leave essential data exposed to unauthorized access and viewing by individuals not connected to the organization. | High | [Test: AC-20(2).1 - Portable Storage Devices]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5 (4)] | [Test: RA-5(4).1 - Discoverable Information]  Not Entered | Failure to ensure that the organization attempts to discern what information about the information system is discoverable by adversaries could result in unauthorized disclosure of information, greater compromise of the system, or to other more severe security threats against the organization. | High | [Test: RA-5(4).1 - Discoverable Information]  Not Entered |  |
| [E-# OR W-#] | Telecommunications Services [NIST 800-53 w/ DHS 4300A CP-8 (3)] | [Test: CP-8(3).1 - Separation Of Primary / Alternate Providers]  Not Entered | Failure to meet the telecommunications services requirements listed below could leave the system vulnerable to environmental risks and other non-operational factors that may cause direct or indirect damage to the working system:  (i) the organization identifies the primary provider's telecommunications service hazards; and (ii) the alternate telecommunications service providers are separated from the primary telecommunications service providers so as not to be susceptible to the same hazards. | High | [Test: CP-8(3).1 - Separation Of Primary / Alternate Providers]  Not Entered |  |
| [E-# OR W-#] | Maintenance Tools [NIST 800-53 w/ DHS 4300A MA-3 (1)] | [Test: MA-3(1).1 - Inspect Tools]  Not Entered | Failure of the organization to inspect all maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel for obvious improper modifications could result in malfunctioning or unstable systems due to uninspected tools and equipment, which could lead eventually to the system losing its integrity. | High | [Test: MA-3(1).1 - Inspect Tools]  Not Entered |  |
| [E-# OR W-#] | Audit Review, Analysis, and Reporting [NIST 800-53 w/ DHS 4300A AU-6 (1)] | [Test: AU-6(1).1 - Process Integration]  Not Entered | Failure of the organization to employ automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process for investigation and response to suspicious activities could result in the loss of the integrity of the system due to untimely detection of threats or attacks. | High | [Test: AU-6(1).1 - Process Integration]  Not Entered |  |
| [E-# OR W-#] | Authenticator Management [NIST 800-53 w/ DHS 4300A IA-5 (3)] | [Test: IA-5(3).1 - In-Person Or Trusted Third-Party Registration]  Not Entered | Failure to meet the authenticator management requirements included below could leave the system vulnerable to unauthorized access, impersonation, and brute force attacks:  (i) the organization defines the types of and/or specific authenticators for which the registration process must be carried out in person before a designated registration authority with authorization by a designated organizational official; and (ii) the organization requires that the registration process to receive organization-defined types of and/or specific authenticators be carried out in person before a designated registration authority with authorization by a designated organizational official (e.g., a supervisor). | High | [Test: IA-5(3).1 - In-Person Or Trusted Third-Party Registration]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (9)] | [Test: IA-2(9).1 - Network Access To Non-Privileged Accounts - Replay Resistant]  Not Entered | Failure to meet the identification and authentication requirements listed below could result in providing any account access to critical or sensitive information:  (i) the organization defines the replay-resistant authentication mechanisms to be used for network access to non-privileged accounts; and (ii) the information system uses the organization-defined replay-resistant authentication mechanisms for network access to non-privileged accounts. | High | [Test: IA-2(9).1 - Network Access To Non-Privileged Accounts - Replay Resistant]  Not Entered |  |
| [E-# OR W-#] | Alternate Storage Site [NIST 800-53 w/ DHS 4300A CP-6 (1)] | [Test: CP-6(1).1 - Separation From Primary Site]  Not Entered | Failure to meet the requirements for alternate storage site listed below could result in a site that is susceptible to the same hazards identified at the primary site, which could lead to the system or the data being unavailable to users:  (i) the contingency plan identifies the primary storage site hazards; and (ii) the alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards identified at the primary site. | High | [Test: CP-6(1).1 - Separation From Primary Site]  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (2)] | [Test: AC-2(2).1 - Removal Of Temporary / Emergency Accounts]  Not Entered | Failure to meet the account management requirements indicated below could result in inaccurate system account audit reports and in rogue temporary and emergency accounts in the system, which could enable would-be attackers to utilize these rogue accounts as access points to the system and consequently launch attack vectors against the entry computer and other neighboring computers:  (i) the information system automatically terminates temporary and emergency accounts after organization-defined time period for each type of account; and, (ii) the organization defines a time period for each type of account after which the information system terminates temporary and emergency accounts. | High | [Test: AC-2(2).1 - Removal Of Temporary / Emergency Accounts]  Not Entered |  |
| [E-# OR W-#] | Incident Reporting [NIST 800-53 w/ DHS 4300A IR-6 (1)] | [Test: IR-6(1).1 - Automated Reporting]  Not Entered | Failure of the organization to employ automated mechanisms to assist in the reporting of security incidents could lead to the organization failing to attend to an incident in a timely manner and eventually losing critical mission/business assets. | High | [Test: IR-6(1).1 - Automated Reporting]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (9)] | [Test: AC-6(9).1 - Auditing Use Of Privileged Functions]  Not Entered | Failure to audit privilege functions could leave the system vulnerable to several risks including access by untrained or unauthorized personnel, improper configuration, or faulty monitoring. | High | [Test: AC-6(9).1 - Auditing Use Of Privileged Functions]  Not Entered |  |
| [E-# OR W-#] | Emergency Power [NIST 800-53 w/ DHS 4300A PE-11] | [Test: PE-11.1 - Emergency Power]  Not Entered | Failure of the organization to provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system or transition of the information system to long-term alternate power in the event of a primary power source loss could lead to the compromise of the system or of the data in the system. | High | [Test: PE-11.1 - Emergency Power]  Not Entered |  |
| [E-# OR W-#] | Media Storage [NIST 800-53 w/ DHS 4300A MP-4 (DHS-3.14.5.f)] | [Test: MP-4(DHS-3.14.5.f) - Rentention of Computer Readable Extracts (CREs)]  Not Entered | Failure to meet the media storage requirements listed below could lead to the compromise of the system or of the data in the system:  (i) ad hoc CREs are destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period;  (ii) permanent erasure of the extracts or the need for continued use of the data is documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC. | High | [Test: MP-4(DHS-3.14.5.f) - Rentention of Computer Readable Extracts (CREs)]  Not Entered |  |
| [E-# OR W-#] | Information System Monitoring [NIST 800-53 w/ DHS 4300A SI-4 (2)] | [Test: SI-4(2).1 - Automated Tools For Real-Time Analysis]  Not Entered | Failure of the organization to employ automated tools to support near-real-time analysis of events could result in the inability to detect in a timely manner any attack on, intrusion of or malicious/abusive use of the information system enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-4(2).1 - Automated Tools For Real-Time Analysis]  Not Entered |  |
| [E-# OR W-#] | Information in Shared Resources [NIST 800-53 w/ DHS 4300A SC-4] | [Test: SC-4.1 - Information in Shared Resources]  Not Entered | Failure of the information system to prevent unauthorized and unintended information transfer via shared system resources could enable an attacker or malicious user to intercept the transfer and gain unauthorized access to critical and sensitive business/mission information. | High | [Test: SC-4.1 - Information in Shared Resources]  Not Entered |  |
| [E-# OR W-#] | Configuration Settings [NIST 800-53 w/ DHS 4300A CM-6 (1)] | [Test: CM-6(1).1 - Automated Central Management / Application / Verification]  Not Entered | Failure of the information system to employ automated mechanisms to centrally manage, apply, and verify configuration settings could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or technology products. | High | [Test: CM-6(1).1 - Automated Central Management / Application / Verification]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8 (1)] | [Test: CM-8(1).1 - Updates During Installations / Removals]  Not Entered | Failure of the organization to update the inventory of information system components as an integral part of component installations could result in misconfigured systems due to the inability to track which integral components need to be installed. | High | [Test: CM-8(1).1 - Updates During Installations / Removals]  Not Entered |  |
| [E-# OR W-#] | Fire Protection [NIST 800-53 w/ DHS 4300A PE-13 (2)] | [Test: PE-13(2).1 - Suppression Devices / Systems]  Not Entered | Failure of the organization employs fire suppression devices/systems for the information system that provide automatic notification of any activation to organization-defined personnel and organization-defined emergency responders could lead to accidents or personnel/employee injury due to the lack of fire suppression devices/systems or due to untimely notification. | High | [Test: PE-13(2).1 - Suppression Devices / Systems]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (1)] | [Test: CP-2(1).1 - Coordinate With Related Plans]  Not Entered | Failure of the organization to coordinate the contingency plan with other related plans (e.g., Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Business Recovery Plan, Incident Response Plan, Emergency Action Plan) could lead to the unavailability of systems that is critical to the overall business processes. | High | [Test: CP-2(1).1 - Coordinate With Related Plans]  Not Entered |  |
| [E-# OR W-#] | Remote Access [NIST 800-53 w/ DHS 4300A AC-17 (1)] | [Test: AC-17(1).1 - Automated Monitoring / Control]  Not Entered | Failure of the information system to employ automated mechanisms to facilitate the monitoring and control of remote access methods could result in a system breach through remote access attack vectors that are not identified in a timely manner. | High | [Test: AC-17(1).1 - Automated Monitoring / Control]  Not Entered |  |
| [E-# OR W-#] | Security Alerts, Advisories, and Directives [NIST 800-53 w/ DHS 4300A SI-5 (1)] | [Test: SI-5(1).1 - Automated Alerts And Advisories]  Not Entered | Failure of the organization to employ automated mechanisms to make security alert and advisory information available throughout the organization as needed could result in the inability to respond to any attack on, intrusion of or unusual/unauthorized use of the information system enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-5(1).1 - Automated Alerts And Advisories]  Not Entered |  |
| [E-# OR W-#] | Non-repudiation [NIST 800-53 w/ DHS 4300A AU-10] | [Test: AU-10.1 - Non-repudiation]  Not Entered | Failure of the information system to provide the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message) could lead to compromise of the system or of the data in the system. | High | [Test: AU-10.1 - Non-repudiation]  Not Entered |  |
| [E-# OR W-#] | Developer Security Testing and Evaluation [NIST 800-53 w/ DHS 4300A SA-11] | [Test: SA-11.1 - Developer Security Testing and Evaluation]  Not Entered | Failure of the organization to require the developer of the information system, system component, or information system service to perform tasks indicated below could leave the system more exposed to vulnerabilities:  (i) Create and implement a security assessment plan that provides for security testing and evaluation:   * at the depth of security-related functional properties, security related externally visible interfaces, high-level design, low-level design, or implementation representation (source code/hardware schematics; and * at the rigor of showing, demonstrating, or rigorously demonstrating;   (ii) Perform unit, integration, system, or regression testing/evaluation at organization-defined breadth/depth;  (iii) Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation;  (iv) Implement a verifiable flaw remediation process; and  (v) Correct flaws identified during security testing/evaluation. | High | [Test: SA-11.1 - Developer Security Testing and Evaluation]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (2)] | [Test: CM-2(2).1 - Automation Support For Accuracy / Currency]  Not Entered | Failure of the organization to employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system could result in a weak security stance of the organization resulting from incomplete or inaccurate configuration that could be applied on a system when there is a need for configuration changes to be implemented. | High | [Test: CM-2(2).1 - Automation Support For Accuracy / Currency]  Not Entered |  |
| [E-# OR W-#] | Media Transport [NIST 800-53 w/ DHS 4300A MP-5 (4)] | [Test: MP-5(4).1 - Cryptographic Protection]  Not Entered | Failure to ensure that the organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas could lead to sensitive information or data to be modified and used by unauthorized users. | High | [Test: MP-5(4).1 - Cryptographic Protection]  Not Entered |  |
| [E-# OR W-#] | Security Impact Analysis [NIST 800-53 w/ DHS 4300A CM-4 (1)] | [Test: CM-4(1).1 - Separate Test Environments]  Not Entered | Failure to meet the security impact analysis requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization analyzes new software in a separate test environment before installation in an operational environment; and (ii) the organization, when analyzing new software in a separate test environment, looks for security impacts due to flaws, weaknesses, incompatibility, or intentional malice. | High | [Test: CM-4(1).1 - Separate Test Environments]  Not Entered |  |
| [E-# OR W-#] | Protection of Audit Information [NIST 800-53 w/ DHS 4300A AU-9 (4)] | [Test: AU-9(4).1 - Access By Subset Of Privileged Users]  Not Entered | Failure to meet the protection of audit information requirements listed below could result in the loss of integrity of the audit information or of the audit tools, which could invalidate any result of forensic investigation:  (i) the organization authorizes access to management of audit functionality to only a limited subset of privileged users; and (ii) the organization protects the audit records of non-local accesses to privileged accounts and the execution of privileged functions. | High | [Test: AU-9(4).1 - Access By Subset Of Privileged Users]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (3)] | [Test: SC-7(3).1 - Access Points]  Not Entered | Failure of the organization to limits the number of external network connections to the information system could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical mission/business assets. | High | [Test: SC-7(3).1 - Access Points]  Not Entered |  |
| [E-# OR W-#] | Flaw Remediation [NIST 800-53 w/ DHS 4300A SI-2 (1)] | [Test: SI-2(1).1 - Central Management]  Not Entered | Failure to ensure that the organization centrally manages the flaw remediation process could result in the ineffective remediation strategy, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-2(1).1 - Central Management]  Not Entered |  |
| [E-# OR W-#] | System Security Plan [NIST 800-53 w/ DHS 4300A PL-2 (3)] | [Test: PL-2(3).1 - Plan / Coordinate With Other Organizational Entities]  Not Entered | Failure to ensure that the organization plans and coordinates security-related activities affecting the information system with organization-defined individuals or groups before conducting such activities in order to reduce the impact on other organizational entities could result in the loss of information. | High | [Test: PL-2(3).1 - Plan / Coordinate With Other Organizational Entities]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (7)] | [Test: SI-7(7).1 - Integration Of Detection And Response]  Not Entered | Failure to ensure that the organization incorporates the detection of unauthorized organization-defined security-relevant changes to the information system into the organizational incident response capability could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical mission/business assets. | High | [Test: SI-7(7).1 - Integration Of Detection And Response]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (1)] | [Test: AC-6(1).1 - Authorize Access To Security Functions]  Not Entered | Failure to meet the least privilege requirements listed below could leave the system vulnerable to unauthorized access:  (i) the organization defines the security functions (deployed in hardware, software, and firmware) and security-relevant information for which access must be explicitly authorized; and (ii) the organization explicitly authorizes access to the organization-defined security functions and security-relevant information. | High | [Test: AC-6(1).1 - Authorize Access To Security Functions]  Not Entered |  |
| [E-# OR W-#] | Information System Backup [NIST 800-53 w/ DHS 4300A CP-9 (3)] | [Test: CP-9(3).1 - Separate Storage For Critical Information]  Not Entered | Failure of the organization to store backup copies of operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software could lead to the disruption of critical mission/business functions, operations, and processes. | High | [Test: CP-9(3).1 - Separate Storage For Critical Information]  Not Entered |  |
| [E-# OR W-#] | Media Sanitization [NIST 800-53 w/ DHS 4300A MP-6 (2)] | [Test: MP-6(2).1 - Equipment Testing]  Not Entered | Failure of the organization to perform test sanitization equipment and procedures to verify correct performance could result in ineffective and untested sanitization equipment causing unpredictable equipment performance, which could lead to the system losing its stability and its integrity. | High | [Test: MP-6(2).1 - Equipment Testing]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan Testing and Exercises [NIST 800-53 w/ DHS 4300A CP-4 (2)] | [Test: CP-4(2).1 - Alternate Processing Site]  Not Entered | Failure of the organization to conduct contingency plan testing at the alternate processing site to familiarize contingency personnel with the facility and its resources and to evaluate the site’s capabilities to support contingency operations could result in the lack of knowledge of the key personnel regarding the facility and its resources, which could leave the site being incapable of supporting the organization's contingency operations. | High | [Test: CP-4(2).1 - Alternate Processing Site]  Not Entered |  |
| [E-# OR W-#] | Telecommunications Services [NIST 800-53 w/ DHS 4300A CP-8 (4)] | [Test: CP-8(4).1 - Provider Contingency Plan]  Not Entered | Failure of the organization to require primary and alternate telecommunications service providers to have contingency plans deemed adequate by the organization could lead to the disruption of critical mission/business functions, operations, and processes due to the ineffective contingency plans for either the primary or the alternate telecommunications service. | High | [Test: CP-8(4).1 - Provider Contingency Plan]  Not Entered |  |
| [E-# OR W-#] | Media Transport [NIST 800-53 w/ DHS 4300A MP-5 (DHS-4.11.f)] | [Test: MP-5(DHS-4.11.f) - Backup Media Shipping]  Not Entered | Failure to ensure that the backup media is shipped using an accountable delivery service (e.g. U.S. Postal Service First Class Mail, Federal Express, United Parcel Service) and properly inventoried could lead to the compromise of the system or of the data in the system. | High | [Test: MP-5(DHS-4.11.f) - Backup Media Shipping]  Not Entered |  |
| [E-# OR W-#] | Auditable Events [NIST 800-53 w/ DHS 4300A AU-2 (3)] | [Test: AU-2(3).1 - Reviews And Updates]  Not Entered | Failure to meet the auditable events requirements listed below could cause difficulty in the general auditing protocols implemented to suit security polices being followed:  (i) the organization defines the frequency of reviews and updates to the list of organization-defined auditable events; and, (ii) the organization reviews and updates the list of organization-defined auditable events in accordance with the organization-defined frequency. | High | [Test: AU-2(3).1 - Reviews And Updates]  Not Entered |  |
| [E-# OR W-#] | Malicious Code Protection [NIST 800-53 w/ DHS 4300A SI-3 (1)] | [Test: SI-3(1).1 - Central Management]  Not Entered | Failure of the organization to centrally manage malicious code protection mechanisms could result in the inability to detect threats/vulnerabilities and exploits identified with and inherent in malicious codes enabling any determined attacker or user to gain unauthorized access to the system, which could eventually lead to the loss of sensitive information or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-3(1).1 - Central Management]  Not Entered |  |
| [E-# OR W-#] | Session Termination [NIST 800-53 w/ DHS 4300A AC-12] | [Test: AC-12.1 - Session Termination]  Not Entered | Failure to terminate a user session when conditions or trigger events have been detected could enable an attacker to try and break into the system and gain access to classified information. | High | [Test: AC-12.1 - Session Termination]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (7)] | [Test: SC-7(7).1 - Prevent Split Tunneling For Remote Devices]  Not Entered | Failure to ensure that the information system, in conjunction with a remote device, prevents the device from simultaneously establishing non-remote connections with the system and communicating via some other connection to resources in external networks could leave the system vulnerable as targets for hackers. | High | [Test: SC-7(7).1 - Prevent Split Tunneling For Remote Devices]  Not Entered |  |
| [E-# OR W-#] | Session Authenticity [NIST 800-53 w/ DHS 4300A SC-23] | [Test: SC-23.1 - Session Authenticity]  Not Entered | Failure to ensure that the information system protects the authenticity of communications sessions could risk the disclosure of sensitive information or the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SC-23.1 - Session Authenticity]  Not Entered |  |
| [E-# OR W-#] | Transmission Integrity [NIST 800-53 w/ DHS 4300A SC-8 (1)] | [Test: SC-8(1).1 - Cryptographic Or Alternate Physical Protection]  Not Entered | Failure to ensure that the information system implements cryptographic mechanisms to prevent unauthorized disclosure of information or detect changes to information during transmission unless otherwise protected by organization-defined alternative physical safeguards could allow an attacker or a malicious user to employ various tactics/strategy to intercept the transmission and gain unauthorized access to critical and sensitive information/data. | High | [Test: SC-8(1).1 - Cryptographic Or Alternate Physical Protection]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (5)] | [Test: SC-7(5).1 - Deny By Default / Allow By Exception]  Not Entered | Failure to ensure that the information system at managed interfaces denies network communications traffic by default and allows network communications traffic by exception (i.e., deny all, permit by exception) could result to undetected unauthorized access. | High | [Test: SC-7(5).1 - Deny By Default / Allow By Exception]  Not Entered |  |
| [E-# OR W-#] | Audit Generation [NIST 800-53 w/ DHS 4300A AU-12 (3)] | [Test: AU-12(3).1 - Changes By Authorized Individuals]  Not Entered | Failure to meet the audit generation requirements listed below could result in the loss of the generated audit data, which could render an audit or forensic investigation efforts useless:  (i) the organization has the ability to extend or limit auditing as necessary to meet organizational requirements; (ii) the organization establishes time thresholds in which audit actions are changed; and, (iii) information system provides the capability for authorized personnel to change organization-defined time thresholds. | High | [Test: AU-12(3).1 - Changes By Authorized Individuals]  Not Entered |  |
| [E-# OR W-#] | Memory Protection [NIST 800-53 w/ DHS 4300A SI-16] | [Test: SI-16.1 - Memory Protection]  Not Entered | Failure to ensure that the information system implements organization-defined security safeguards to protect its memory from unauthorized code execution could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical mission/business assets. | High | [Test: SI-16.1 - Memory Protection]  Not Entered |  |
| [E-# OR W-#] | Access Control for Transmission Medium [NIST 800-53 w/ DHS 4300A PE-4] | [Test: PE-4.1 - Access Control for Transmission Medium]  Not Entered | Failure of the organization to control physical access to organization-defined information system distribution and transmission lines within organizational facilities could result in the disclosure of information. | High | [Test: PE-4.1 - Access Control for Transmission Medium]  Not Entered |  |
| [E-# OR W-#] | Maintenance Tools [NIST 800-53 w/ DHS 4300A MA-3 (2)] | [Test: MA-3(2).1 - Inspect Media]  Not Entered | Failure of the organization to check all media containing diagnostic test programs (e.g., software or firmware used for information system maintenance or diagnostics) for malicious code before the media are used in the information system could lead eventually to the system losing its integrity or its stability. | High | [Test: MA-3(2).1 - Inspect Media]  Not Entered |  |
| [E-# OR W-#] | Controlled Maintenance [NIST 800-53 w/ DHS 4300A MA-2 (2)] | [Test: MA-2(2).1 - Automated Maintenance Activities]  Not Entered | Failure to meet the automated maintenance activity requirements listed below could lead eventually to the system losing its stability or its integrity:  (i) the organization employs automated mechanisms to schedule, conduct, and document maintenance and repairs; and (ii) the organization produces up-to date, accurate, and complete records of all maintenance and repair actions requested, scheduled, in process, and completed. | High | [Test: MA-2(2).1 - Automated Maintenance Activities]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (21)] | [Test: SC-7(21).1 - Isolation Of Information System Components]  Not Entered | Failure to ensure that the organization employs boundary protection mechanisms to separate organization-defined information system components supporting organization defined missions and/or business functions could leave the system vulnerable to improper utilization of resources due to unmonitored activity of access. | High | [Test: SC-7(21).1 - Isolation Of Information System Components]  Not Entered |  |
| [E-# OR W-#] | Wireless Access [NIST 800-53 w/ DHS 4300A AC-18 (5)] | [Test: AC-18(5).1 - Antennas / Transmission Power Levels]  Not Entered | Failure to meet the antenna/transmission power level requirements listed below could leave the system vulnerable to risks brought about by wireless data transmissions:  (i) the organization limits unauthorized use of wireless communications outside of organization-controlled boundaries; (ii) the organization conducts periodic wireless surveys prior to limiting unauthorized use of wireless communications outside of organization-controlled boundaries; and, (iii) the organization selects radio antennas and calibrates transmission power levels to reduce the probability that usable signals can be received outside of organization-controlled boundaries. | High | [Test: AC-18(5).1 - Antennas / Transmission Power Levels]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (3)] | [Test: CP-2(3).1 - Resume Essential Missions / Business Functions]  Not Entered | Failure to meet the contingency plan requirements listed below could lead to the unavailability of systems that is critical to the overall business processes:  (i) the organization defines the time period for planning the resumption of essential missions and business functions as a result of contingency plan activation; and (ii) the organization plans for the resumption of essential missions and business function within organization-defined time period of contingency plan activation. | High | [Test: CP-2(3).1 - Resume Essential Missions / Business Functions]  Not Entered |  |
| [E-# OR W-#] | Spam Protection [NIST 800-53 w/ DHS 4300A SI-8 (1)] | [Test: SI-8(1).1 - Central Management]  Not Entered | Failure of the organization to centrally manage spam protection mechanisms leaves the organization with unreliable and unsafe/unprotected information system, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-8(1).1 - Central Management]  Not Entered |  |
| [E-# OR W-#] | Acquisitions [NIST 800-53 w/ DHS 4300A SA-4 (2)] | [Test: SA-4(2).1 - Design / Implementation Information For Security Controls]  Not Entered | Failure to ensure that the organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes security-relevant external system interfaces, high-level design, low-level design, source code/hardware schematics, or organization-defined level of detail could result in the acquisition of inherently unsafe/non-secure systems that would expose the organization to other exploits and threats/vulnerabilities, which could eventually lead to the loss of critical mission/business assets or to the disruption of organization operations, functions and services. | High | [Test: SA-4(2).1 - Design / Implementation Information For Security Controls]  Not Entered |  |
| [E-# OR W-#] | Security Awareness [NIST 800-53 w/ DHS 4300A AT-2 (2)] | [Test: AT-2(2).1 - Insider Threat]  Not Entered  Not Entered  Not Entered | Failure to ensure that the organization includes security awareness training on recognizing and reporting potential indicators of insider threat could result in the organization's personnel's inability to communicate employee and management concerns regarding insider threats. | High | [Test: AT-2(2).1 - Insider Threat]  Not Entered  Not Entered  Not Entered |  |
| [E-# OR W-#] | Account Management [NIST 800-53 w/ DHS 4300A AC-2 (3)] | [Test: AC-2(3).1 - Disable Inactive Accounts]  Not Entered | Failure to meet the account management requirements indicated below could result in an inaccurate audit report and could enable an intruder to utilize the inactive accounts as access points to the system:  (i) the organization defines in a time period after which the information system disables inactive accounts; and (ii) the information system automatically disables inactive accounts after organization-defined time period. | High | [Test: AC-2(3).1 - Disable Inactive Accounts]  Not Entered |  |
| [E-# OR W-#] | Developer Configuration Management [NIST 800-53 w/ DHS 4300A SA-10] | [Test: SA-10.1 - Developer Configuration Management]  Not Entered | Failure to meet the developer configuration management requirements listed below could lead to instability of the system or possibly to the compromise of the system:  (i) perform configuration management during information system:   * design; * development; * implementation; and * operation;   (ii) manage and control changes to the information system during:   * design; * development; * implementation; and * modification;   (iii) implement only organization-approved changes; (iv) document approved changes to the information system; and (v) track security flaws and flaw resolution. | High | [Test: SA-10.1 - Developer Configuration Management]  Not Entered |  |
| [E-# OR W-#] | Automated Notification [NIST 800-53 w/ DHS 4300A PS-4 (2)] | [Test: PS-4(2).1 - Automated Notification]  Not Entered | Failure to ensure that the organization employs automated mechanisms to notify organization-defined personnel or roles upon termination of an individual could risk data being compromised by such individuals. | High | [Test: PS-4(2).1 - Automated Notification]  Not Entered |  |
| [E-# OR W-#] | Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7 (4)] | [Test: CP-7(4).1 - Preparation For Use]  Not Entered | Failure to ensure that the alternate processing site is configured to support the minimum required information system operational capability and is ready to use as the operational site could lead to the inability to restore business operations/processes in a timely fashion. | High | [Test: CP-7(4).1 - Preparation For Use]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (8)] | [Test: SC-7(8).1 - Route Traffic To Authenticated Proxy Servers]  Not Entered | Failure to ensure that the information system routes organization-defined internal communications traffic to organization-defined external networks through authenticated proxy servers at managed interfaces could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical mission/business assets. | High | [Test: SC-7(8).1 - Route Traffic To Authenticated Proxy Servers]  Not Entered |  |
| [E-# OR W-#] | Incident Handling [NIST 800-53 w/ DHS 4300A IR-4 (4)] | [Test: IR-4(4).1 - Information Correlation]  Not Entered | Failure to ensure that the organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response could prevent the immediate restoration of the system into its stable working state should an attack occur. | High | [Test: IR-4(4).1 - Information Correlation]  Not Entered |  |
| [E-# OR W-#] | Least Privilege [NIST 800-53 w/ DHS 4300A AC-6 (10)] | [Test: AC-6(10).1 - Prohibit Non-Privileged Users From Executing Privileged Functions]  Not Entered | Failure to prevent non-privileged users from executing privileged functions could leave the system vulnerable to several risks including access by untrained or unauthorized personnel, improper configuration, or faulty monitoring. | High | [Test: AC-6(10).1 - Prohibit Non-Privileged Users From Executing Privileged Functions]  Not Entered |  |
| [E-# OR W-#] | Vulnerability Scanning [NIST 800-53 w/ DHS 4300A RA-5 (2)] | [Test: RA-5(2).1 - Update By Frequency / Prior To New Scan / When Identified]  Not Entered | Failure to meet the vulnerability scanning requirement listed below could put the organization in weaker security posture that could result in unauthorized disclosure of information, greater compromise of the system, or to other more severe security threats against the organization:  (i) the organization defines the frequency of updates for information system vulnerabilities scanned; and (ii) the organization updates the list of information system vulnerabilities scanned in accordance with the organization-defined frequency or when new vulnerabilities are identified and reported. | High | [Test: RA-5(2).1 - Update By Frequency / Prior To New Scan / When Identified]  Not Entered |  |
| [E-# OR W-#] | Protection of Audit Information [NIST 800-53 w/ DHS 4300A AU-9 (3)] | [Test: AU-9(3).1 - Cryptographic Protection]  Not Entered | Failure to ensure that the information system uses cryptographic mechanisms to protect the integrity of audit information and audit tools could result in the loss of integrity of the audit information or of the audit tools, which could invalidate any result of forensic investigation. | High | [Test: AU-9(3).1 - Cryptographic Protection]  Not Entered |  |
| [E-# OR W-#] | Penetration Testing [NIST 800-53 w/ DHS 4300A CA-8] | [Test: CA-8.1 - Penetration Testing]  Not Entered | Failure to meet the penetration testing requirements listed below could lead to compromise of the system or of the data in the system:  (i) the organization conducts penetration testing in an organizational-defined frequency; (ii) the organization conducts penetration testing on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries; (iii) the organization follows standard penetration testing methods:   * pretest analysis based on full knowledge of the target system; * pretest identification of potential vulnerabilities based on pretest analysis; and, * testing designed to determine exploitability of identified vulnerabilities.   (iv) the organization agrees the rules of engagement before commencing penetration testing scenarios; | High | [Test: CA-8.1 - Penetration Testing]  Not Entered |  |
| [E-# OR W-#] | Information System Recovery and Reconstitution [NIST 800-53 w/ DHS 4300A CP-10 (2)] | [Test: CP-10(2).1 - Transaction Recovery]  Not Entered | Failure to ensure that the information system implements transaction recovery for systems that are transaction-based could compromise data integrity and availability, should a system go down unexpectedly. | High | [Test: CP-10(2).1 - Transaction Recovery]  Not Entered |  |
| [E-# OR W-#] | Monitoring Physical Access [NIST 800-53 w/ DHS 4300A PE-6 (4)] | [Test: PE-6(4).1 - Monitoring Physical Access To Information Systems]  Not Entered | Failure to ensure that the organization monitors physical access to the information system in addition to the physical access monitoring of the facility as organization-defined physical spaces containing one or more components of the information system could lead to computer facilities and resources from espionage, sabotage, damage, and theft. | High | [Test: PE-6(4).1 - Monitoring Physical Access To Information Systems]  Not Entered |  |
| [E-# OR W-#] | Incident Handling [NIST 800-53 w/ DHS 4300A IR-4 (1)] | [Test: IR-4(1).1 - Automated Incident Handling Processes]  Not Entered | Failure of the organization to employ automated mechanisms to support the incident handling process could leave the organization unable to respond to an incident in a timely manner, leading to the disruption of critical mission/business operations. | High | [Test: IR-4(1).1 - Automated Incident Handling Processes]  Not Entered |  |
| [E-# OR W-#] | Boundary Protection [NIST 800-53 w/ DHS 4300A SC-7 (4)] | [Test: SC-7(4).1 - External Telecommunications Services]  Not Entered | Failure to meet the requirements of boundary protection indicated below could permit an attacker or a malicious user to gain unauthorized access to the system or data and could risk the loss of critical mission/business assets:  (i) the organization implements a managed interface for each external telecommunication service;  (ii) the organization establishes a traffic flow policy for each managed interface;  (iii) the organization protects the confidentiality and integrity of the information being transmitted across each interface;  (iv) the organization documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; and  (v) the organization reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency] and removes exceptions that are no longer supported by an explicit mission/business need. | High | [Test: SC-7(4).1 - External Telecommunications Services]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8 (5)] | [Test: CM-8(5).1 - No Duplicate Accounting Of Components]  Not Entered | Failure to ensure that the organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system could eventually lead to the loss of critical resources due to the absence of tracking process that could detect missing critical components in a timely fashion. | High | [Test: CM-8(5).1 - No Duplicate Accounting Of Components]  Not Entered |  |
| [E-# OR W-#] | Software and Information Integrity [NIST 800-53 w/ DHS 4300A SI-7 (1)] | [Test: SI-7(1).1 - Integrity Checks]  Not Entered | Failure to ensure that the information system performs an integrity check of organization-defined software, firmware, and information at startup, organization-defined transitional states / security-relevant events, or organization-defined frequency could result in an unreliable information system, which could eventually lead to the loss of organizational assets or to the disruption of critical mission/business functions, services, and operations/processes. | High | [Test: SI-7(1).1 - Integrity Checks]  Not Entered |  |
| [E-# OR W-#] | Rules of Behavior [NIST 800-53 w/ DHS 4300A PL-4 (1)] | [Test: PL-4(1).1 - Social Media And Networking Restrictions]  Not Entered | Failure to ensure that the organization includes in the rules of behavior, explicit restrictions on the use of social media/networking sites and posting information on commercial websites could lead to the user inadvertently abusing the information system resources. | High | [Test: PL-4(1).1 - Social Media And Networking Restrictions]  Not Entered |  |
| [E-# OR W-#] | Fire Protection [NIST 800-53 w/ DHS 4300A PE-13 (3)] | [Test: PE-13(3).1 - Automatic Fire Suppression]  Not Entered | Failure of the organization to employ an automatic fire suppression capability in facilities that are not staffed on a continuous basis could risk damage to the facilities, systems, and data/information, which could lead to the disruption of critical mission/business operations. | High | [Test: PE-13(3).1 - Automatic Fire Suppression]  Not Entered |  |
| [E-# OR W-#] | Access Records [NIST 800-53 w/ DHS 4300A PE-8 (1)] | [Test: PE-8(1).1 - Automated Records Maintenance / Review]  Not Entered | Failure of the organization to employ automated mechanisms to facilitate the maintenance and review of access records could result in the untimely detection of unauthorized access, which could lead to the complete compromise of the system or the information in the system. | High | [Test: PE-8(1).1 - Automated Records Maintenance / Review]  Not Entered |  |
| [E-# OR W-#] | Timely Maintenance [NIST 800-53 w/ DHS 4300A MA-6] | [Test: MA-6.1 - Timely Maintenance]  Not Entered | Failure to meet the timely maintenance requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization defines security-critical information system components and/or key information technology components for which it will obtain maintenance support and/or spare parts; (ii) the organization defines the time period within which support and/or spare parts must be obtained after a failure; and (iii) the organization obtains maintenance support and/or spare parts for the organization-defined list of security-critical information system components and/or key information technology components within the organization-defined time period of failure. | High | [Test: MA-6.1 - Timely Maintenance]  Not Entered |  |
| [E-# OR W-#] | Contingency Plan [NIST 800-53 w/ DHS 4300A CP-2 (5)] | [Test: CP-2(5).1 - Continue Essential Missions / Business Functions]  Not Entered | Failure to meet the contingency plan requirements listed below could weaken the overall security posture of the system:  (i) the organization plans for the continuance of essential missions and business functions with little or no loss of operational continuity; and (ii) the organization sustains operational continuity until full information system restoration at primary processing and/or storage sites. | High | [Test: CP-2(5).1 - Continue Essential Missions / Business Functions]  Not Entered |  |
| [E-# OR W-#] | Configuration Change Control [NIST 800-53 w/ DHS 4300A CM-3 (DHS-2.1.8.g)] | [Test: CM-3(DHS-2.1.8.g) - Timely Response to ICCB]  Not Entered | Failure of the ISSO to ensure timely responses to Infrastructure Change Control Board (ICCB) change request packages could leave the system vulnerable to unexpected instability in operation. | High | [Test: CM-3(DHS-2.1.8.g) - Timely Response to ICCB]  Not Entered |  |
| [E-# OR W-#] | Least Functionality [NIST 800-53 w/ DHS 4300A CM-7 (5)] | [Test: CM-7(5).1 - Authorized Software / Whitelisting]  Not Entered | Failure to meet the white listing requirements listed below could leave the system vulnerable to attacks and denial-of-service conditions:  (i) the organization identifies software programs authorized to execute on the information system; (ii) the organization employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system; and, (iii) the organization reviews and updates the list of authorized software programs on an organization-defined frequency. | High | [Test: CM-7(5).1 - Authorized Software / Whitelisting]  Not Entered |  |
| [E-# OR W-#] | Baseline Configuration [NIST 800-53 w/ DHS 4300A CM-2 (1)] | [Test: CM-2(1).1 - Reviews And Updates]  Not Entered | Failure of the organization to update the baseline configuration of the information system as an integral part of information system component installations could result in a weak security stance of the organization due to the untimely detection of misconfigured systems or of systems that need configuration updates:  (i) the organization defines:   * the frequency of reviews and updates to the baseline configuration of the information system; and * the circumstances that require reviews and updates to the baseline configuration of the information system; and   (ii) the organization reviews and updates the baseline configuration of the information system   * in accordance with the organization-defined frequency; * when required due to organization-defined circumstances; and * as an integral part of information system component installations and upgrades. | High | [Test: CM-2(1).1 - Reviews And Updates]  Not Entered |  |
| [E-# OR W-#] | Alternate Processing Site [NIST 800-53 w/ DHS 4300A CP-7 (1)] | [Test: CP-7(1).1 - Separation From Primary Site]  Not Entered | Failure to meet the requirements for alternate processing site indicated below could result in the system or data being unavailable when needed or, possibly, could lead to the discontinuation of the entire business operations/processes:  (i) the contingency plan identifies the primary processing site hazards; and (ii) the alternate processing site is separated from the primary processing site so as not to be susceptible to the same hazards identified at the primary site. | High | [Test: CP-7(1).1 - Separation From Primary Site]  Not Entered |  |
| [E-# OR W-#] | Access Restrictions for Change [NIST 800-53 w/ DHS 4300A CM-5 (2)] | [Test: CM-5(2).1 - Review System Changes]  Not Entered | Failure to meet the access restrictions for change requirements listed below could allow any user to effect system wide modification without being detected in a timely manner and cause the system to be unstable or lose its integrity:  (i) the organization defines the frequency for conducting audits of information system changes; and (ii) the organization conducts audits of information system changes in accordance with the organization-defined frequency and when indications so warrant to determine whether unauthorized changes have occurred. | High | [Test: CM-5(2).1 - Review System Changes]  Not Entered |  |
| [E-# OR W-#] | Contingency Training [NIST 800-53 w/ DHS 4300A CP-3 (1)] | [Test: CP-3(1).1 - Simulated Events]  Not Entered | Failure of the contingency training material to address the procedures and activities necessary to fulfill identified organizational contingency roles and responsibilities could lead to the compromise of the system or of the data in the system:  (i) the organization incorporates simulated events into contingency training; and (ii) the incorporation of simulated events into contingency training facilitates effective response by personnel in crisis situations. | High | [Test: CP-3(1).1 - Simulated Events]  Not Entered |  |
| [E-# OR W-#] | Wireless Access [NIST 800-53 w/ DHS 4300A AC-18 (4)] | [Test: AC-18(4).1 - Restrict Configurations By Users]  Not Entered | Failure to meet the user configuration restriction requirements indicated below could result in a number of unmanaged and unauthorized wireless access to the information system:  (i) the organization employs access enforcement mechanisms when allowing users to configure wireless networking capabilities; and, (ii) the organization identifies and authorizes users who are allowed to independently configure wireless networking capabilities. | High | [Test: AC-18(4).1 - Restrict Configurations By Users]  Not Entered |  |
| [E-# OR W-#] | Alternate Work Site [NIST 800-53 w/ DHS 4300A PE-17] | [Test: PE-17.1 - Alternate Work Site]  Not Entered | Failure to meet the alternate work site requirements listed below could lead to the compromise of the system or of the data in the system:  (i) the organization employs organization-defined security controls at alternate work sites; (ii) the organization assesses as feasible, the effectiveness of security controls at alternate work sites; and, (iii) the organization provides a means for employees to communicate with information security personnel in case of security incidents or problems. | High | [Test: PE-17.1 - Alternate Work Site]  Not Entered |  |
| [E-# OR W-#] | Incident Response Testing and Exercises [NIST 800-53 w/ DHS 4300A IR-3 (2)] | [Test: IR-3(2).1 - Coordination With Related Plans]  Not Entered | Failure to meet the incident response testing requirements listed below could result in the inability to respond properly to an incident and in a timely manner, which could lead to the disruption of critical mission/business functions, operations, and processes:  (i) the organization provides the following organizational plans related to incident response testing;   * Business Continuity Plans * Contingency Plans * Disaster Recovery Plans * Continuity of Operations Plans * Crisis Communications Plans * Critical Infrastructure Plans * Occupant Emergency Plans   (ii) the organization coordinates incident response testing with organizational elements responsible for related plans. | High | [Test: IR-3(2).1 - Coordination With Related Plans]  Not Entered |  |
| [E-# OR W-#] | Information System Component Inventory [NIST 800-53 w/ DHS 4300A CM-8 (2)] | [Test: CM-8(2).1 - Automated Maintenance]  Not Entered | Failure of the organization to employ automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components could eventually lead to the loss of critical resources due to the absence of tracking process that could detect missing critical components in a timely fashion. | High | [Test: CM-8(2).1 - Automated Maintenance]  Not Entered |  |
| [E-# OR W-#] | Physical Access Control [NIST 800-53 w/ DHS 4300A PE-3 (1)] | [Test: PE-3(1).1 - Information System Access]  Not Entered | Failure to ensure that the organization enforces physical access authorizations to the information system in addition to the physical access controls for the facility at organization-defined physical spaces containing one or more components of the information system could result in access control system lacking effective physical protection, which could lead to the disclosure of sensitive information or to the disruption of critical mission/business functions, operations, and processes. | High | [Test: PE-3(1).1 - Information System Access]  Not Entered |  |
| [E-# OR W-#] | Non-Local Maintenance [NIST 800-53 w/ DHS 4300A MA-4 (2)] | [Test: MA-4(2).1 - Document Nonlocal Maintenance]  Not Entered | Failure of the organization to address the installation and use of remote maintenance and diagnostic links in the security plan for the information system could lead to the system losing its integrity and stability or to the critical information/data being disclosed. | High | [Test: MA-4(2).1 - Document Nonlocal Maintenance]  Not Entered |  |
| [E-# OR W-#] | Access Restrictions for Change [NIST 800-53 w/ DHS 4300A CM-5] | [Test: CM-5.1 - Access Restrictions for Change]  Not Entered | Failure to ensure that the organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system could lead to the compromise of the system or of the data in the system: | High | [Test: CM-5.1 - Access Restrictions for Change]  Not Entered |  |
| [E-# OR W-#] | Identification and Authentication (Organizational Users) [NIST 800-53 w/ DHS 4300A IA-2 (11)] | [Test: IA-2(11).1 - Remote Access - Separate Device]  Not Entered | Failure to ensure that the information system implements multifactor authentication for remote access to privileged and non-privileged accounts could result in providing any account access to critical or sensitive information. | High | [Test: IA-2(11).1 - Remote Access - Separate Device]  Not Entered |  |
| [E-# OR W-#] | Content of Audit Records [NIST 800-53 w/ DHS 4300A AU-3 (1)] | [Test: AU-3(1).1 - Additional Audit Information]  Not Entered | Failure of the information system to provide the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject could result in incomplete data critical to the success of a forensic process, which could lead to untimely detection of any attack on the system:  (i) the organization defines the additional, more detailed information to be included in audit records for audit events identified by type, location, or subject; and, (ii) the information system includes the organization-defined additional, more detailed information in the audit records for audit events identified by type, location, or subject. | High | [Test: AU-3(1).1 - Additional Audit Information]  Not Entered |  |

**Table 3-2: Risks Recommended be Remediated via POA&M within Six Months of ATO**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Traceability | Risks | Affected Elements | Risk Level | Recommended Remediation | Compensating Measure |  |
| There are no Risks that need to be Remediated via POAM within Six Months of ATO | | | | | | |

**Table 3-3: Acceptable Risks**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Traceability | Risks | Affected Elements | Risk Level | Recommended Remediation | Compensating Measure |  |
| There is no Acceptable Risk defined | | | | | | |

## 3.1 Statement of Residual Risk

{enter your statement of risidual risk here}

## 3.2 Level of Acceptable Risk

Among the 30 identified, [PERCENTAGE OF VULNERABILITIES CONSIDERED UNACCEPTABLE] are considered unacceptable because serious harm could result and affect the operation of the system. Immediate, mandatory countermeasures need to be implemented to mitigate the risk of these threats. Resources must be made available to reduce the risk to an acceptable level.   
  
[PERCENTAGE OF VULNERABILITIES CONSIDERED ACCEPTABLE] of the identified vulnerabilities are considered acceptable to the system because only minor problems may result from these risks. Recommended countermeasures have also been provided for implementation to reduce or eliminate the risk.

**Table 3-4: Risk Level of Acceptable/Unacceptable Vulnerabilities**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **High** | **Moderate** | **Low** |
| Unacceptable | [#] | [#] | [#] |
| Acceptable | [#] | [#] | [#] |

## 3.3 Security Control Assessor Recommendation to AO

After evaluating the results of the security assessment, it is my opinion as the Security Control Assessor that an [ACCEPTABLE/UNACCEPTABLE] level of risk to the agency exists and I recommend to the AO that the system [SHOULD/SHOULD NOT] be authorized to operate.   
[ADDITIONAL COMMENTS]   
  
[SIGNATURE & DATE]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date