Homeland Security

DHS Policy Directive 4300A
"*Information Technology System Security Program, Sensitive Systems*"

Attachment AA

Cybersecurity Service Provider (CSP) Program

Version 2.1
September 13, 2022

Document Change History

Version	Date	Description
1.0	May 6, 2022	Initial release by Ron Freeman, CISOD
2.0	July 25, 2022	Edits provided by CBP, USCIS, and FEMA and adjudicated by DHS OCIO CISOD Office of Policy, C Santangelo
2.1	September 13, 2022	Minor edits to revise alignment of some oversight responsibilities to the DHS DCIO council. A. Scimemi

Contents

This page intentionally blank

INTRODUCTION

In support of Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure" and the resulting Security Operations Center (SOC) Optimization Plan, the Department of Homeland Security formed under the direction of the DHS CIO a Cybersecurity Services Provider (CSP) Assessment Program. This program is modeled after the Joint Force Headquarters Department of Defense Information Networks (JFHQ-DoDIN) program for evaluating the effectiveness of critical cybersecurity services. The Department will assess all Component Security Operations Centers (SOC) against the DHS CSP Framework maturity standards as set forth and managed by the DHS CISO Council. Additionally, the benefits of this program provide enduring support to Executive Order 14028, "Improving the Nation's Cybersecurity."

The DHS CSP Program will also inspect DHS and all Component Network Operations Centers (NOC) against the DHS CSP NOC Framework Evaluator Scoring Metrics (ESM) standards as approved and governed by the DHS DCIO Council. Those organizations that meet the minimum standard as defined by the DHS CSP Program will be deemed an Accredited SOC or NOC and be able to provide services to their Component, but not offer services to other DHS Components. Organizations that exceed the minimum standard and meet the set of enhanced maturity criteria as defined by the program will be accredited as a Center of Excellence (COE). The entity is then eligible to provide cybersecurity service offerings to other DHS Components.

Component SOCs and NOCs receiving these designations will be inspected every three (3) years and will be assessed against all approved CSP Metrics each time. Additionally, all Component Subscribers (those purchasing services from CSPs) will also be assessed every three (3) years against all metrics to ensure the services received are meeting the required Maturity Levels.

To ensure a standard level of capabilities across DHS Cybersecurity Services, DHS will implement, with these goals, a Cybersecurity Services Inspection and Accreditation Program to:

- Ensure a standard level of cybersecurity services capabilities across DHS.
- Establish a shared services model that promotes effective use of limited resources.
- Incorporate program enhancements and requirements to improve cybersecurity services maturity levels and capabilities.

1.0 BACKGROUND

The DHS Cybersecurity Service Provider model is a collaborative DHS framework that elevates the overall enterprise cybersecurity posture in terms of security capabilities (inclusive of security controls, practices, functions, technologies, and personnel). The DHS Cybersecurity Services Program (CSP) serves as the tool that DHS and its Components use to conduct assessments for Operations Centers to provide services for IT Information Systems within their Components, as well as IT Information Systems of other Components within DHS. The requirements within this document are baseline capabilities and services required of all DHS Components.

1.1 Purpose

This document provides information for Department of Homeland Security (DHS) Components and other entities within its purview policy, guidance, and information on the DHS Cybersecurity Services Program (CSP). The CSP Program was developed to assess the maturity of Component/Organization's Security and Network Operation Centers. The DHS CSP Program will be expanded in FY23 to include cloud platform maturity assessments.

1.2 References

Federal Laws

- Executive Order 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"
- Federal Cybersecurity Risk Determination Report and Action Plan, May 2018
- Report to the President on Federal IT Modernization, American Technology Council (ATC), December 2017

Department of Homeland Security Publications

- DHS Cybersecurity Operation Center CONOPS
- 4300A – The Sensitive Systems Handbook
- DHS Cybersecurity Service Provider Policy Memo
- DHS Cybersecurity Service Provider Program Addendum

2.0 CSP POLICY STATEMENTS

The following policy statements apply to the implementation of component-level SOCs, and NOCs as initially established in the DHS Cybersecurity Service Provider Program Addendum signed by the DHS Chief Information Officer and CSP Authorizing Official (AO):

1. All DHS Component SOCs and NOCs must pass a formal assessment and receive a designation of either Accredited or Center of Excellence (COE). COEs are authorized to provide services on a fee basis to other DHS components while accredited organizations are authorized to provide services to their Component and associated systems. Components that fail to achieve these designations are unaccredited and must subscribe to the services of a COE SOC or NOC from within the Department of Homeland Security.

   SOCs or NOCs that do not meet the required maturity to be accredited shall submit a remediation plan within 30 days from the assessment. Upon mitigation of the identified deficiencies, the CSP assessment team will re-evaluate failed metrics within 90 days. The remediation timelines will be approved by the CSP Assessment Team and Program Management Office (PMO). Components that fail to meet the requirements after re-evaluation must procure services from a COE within 6 months or otherwise as determined by the DHS CIO.

2. Both Providers and Subscribers, will be inspected at least every three (3) years or when Providers or Subscribers revise their service agreements. Additionally, all Component Subscribers will be assessed alongside their Provider's anniversary date to ensure the services received are meeting the required maturity. Assessment durations are 1 to 2 weeks depending on Component Subject

Matter Expert (SME) schedules and the quality of the pre-assessment package, due 30 days prior to the inspection date.

3. All DHS Federal Information Security Modernization Act (FISMA) systems, whether government or commercially hosted, owned, or operated, are required to obtain SOC or NOC services from a DHS accredited SOC or NOC. SOC and NOC services obtained from or provided by a commercial provider or hosting environment do not meet this policy requirement. In cases where individual systems cannot be made compliant with this policy, a formal policy waiver shall be submitted to the DHS Chief Information Officer (CIO) prior to procurement activities. In the event a waiver is granted, recurring cyber hygiene assessments will be required from the commercial provider performing SOC functions.

4. DHS Components are prohibited from outsourcing SOC or NOC services in their entirety to commercial providers. Accordingly, the DHS CSP program management office will not evaluate for accreditation commercial vendors seeking to provide SOC-as-a-Service or NOC-as-a-Service to DHS Components or Offices. SOC and NOC operations are inherently governmental functions which cannot be assigned or delegated to a non-government organization. Support staff obtained through contracts with commercial providers is expected and authorized. Any support staff obtained in this manner shall not fill government leadership roles in the execution of the functions and processes outlined in the SOC or NOC standards framework.

5. The DHS CIO assumes the role as the DHS CSP Authorizing Official (AO) and with it the authority to implement and manage all aspects of the DHS Cybersecurity Services Program. The AO has the authority to delegate the governance of the DHS CSP Program to the DHS DCIO Council. The approval or denial of accreditation is determined by the AO or their designee, based on the DHS CSP Assessment Team recommendation, described in the DHS Cybersecurity Operations Concept of Operations. The AO will accept the risk associated with the accreditation decision.

6. The DHS CSP Program will expand to include Cloud Platform Assessments in FY 23. The CSP PMO will develop and distribute the framework in FY 2022 in support of assessment events scheduled for the following fiscal year.

3.0 CSP ASSESSMENT PROCESS

The cybersecurity service provider evaluation process is based on a four-phase lifecycle approach ultimately leading to the authorization of cybersecurity services for DHS Component organizations. The cybersecurity service evaluation process provides DHS with a standardized means to assess an organization directing and managing network operations and cybersecurity activities and supporting CSPs based on identified performance criteria best practices, self-assessment tools, and DHS requirements in the DHS Cybersecurity Services Evaluator Scoring Metrics (ESM).

The DHS CSP service evaluation and validation processes begin with the submission of a formal CSP Assessment Package to the cybersecurity service evaluators. DHS, its Components, and service providers should have detailed knowledge of the criteria in this document before submitting a CSP Assessment Package. The CSP Assessment Package should contain a letter of

request for evaluation and/or validation of cybersecurity services; a completed self-assessment conducted using this ESM and all supporting documentation applicable to their cybersecurity operations. The CSP Assessment Package with self-assessment is reviewed by the cybersecurity service evaluators to determine readiness for a formal, on-site evaluation for authorization to provide cybersecurity services for DHS IT Information Systems (IS). The self- assessment and CSP Assessment Package review provides input to the formal on-site evaluation, where the authorization recommendation and overall cybersecurity program effectiveness is determined.

The four-phase process is displayed in the diagram and described below:

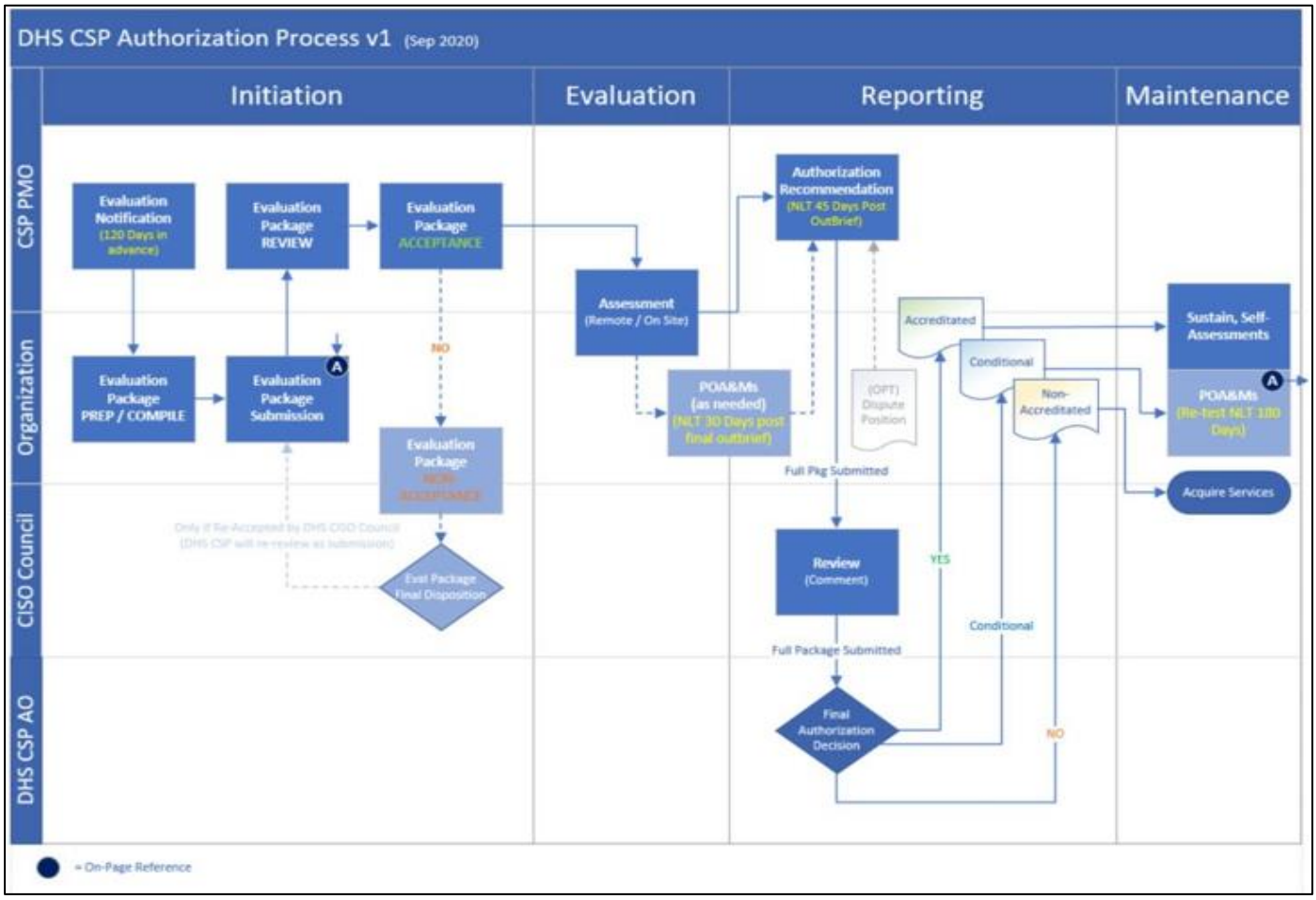

Figure 1: CSP SOC Assessment Testing Process (High Level)

3.1 Phase 1 – Initiation

The Initiation Phase commences the three-year cycle for the cybersecurity service evaluation process. The activities in the Initiation Phase compile the information necessary for identifying cybersecurity service alignment, supporting documentation for cybersecurity services performed and a DHS Cybersecurity Services ESM self-assessment.

The Initiation Phase consists of four activities:

1. Evaluation Notification – The DHS CSP PMO is responsible for notifying each cybersecurity services entity to be assessed 90 days in advance of its scheduled evaluation. The evaluation notification will include all requirements and directions for submission of a CSP evaluation package.
2. Evaluation Package Submission – Prior to its scheduled evaluation, each organization to be

assessed is responsible for submitting and/or updating a self-evaluation package to the DHS CSP PMO for the assessment team/evaluators to review. The evaluation package contains all documentation applicable to cybersecurity service operations and this process. For any classified documentation, the assessed organization will submit a POC with phone number and e-mail address that will provide the information via secure channels, when requested.

3. Evaluation Package Review – DHS CSP Program personnel are assigned to review, analyze, and discuss all furnished documentation. The number of DHS CSP evaluators assigned will vary depending on the organization size, scope of services being evaluated, and classification of the data handled. If an evaluation package contains insufficient documentation, the lead DHS CSP evaluator will coordinate with the assessed organization to resolve any deficiencies.
4. Evaluation Package Acceptance – Phase 1 concludes with the acceptance by the DHS CSP PMO of the evaluation package. If the package is accepted, it will continue the evaluation process and the CSP PMO will coordinate with the organization to schedule on-site evaluation. As part of the acceptance, the DHS CSP PMO may require the assessed entity to implement corrective actions, typically by a specific date, regarding the self-assessment results and specific performance metrics before the on-site evaluation. If the entity/component already has been scheduled, this date will be adjusted to allow time to implement appropriate corrective actions. This will be monitored by the DHS CSP PMO and reported, as appropriate, to the DHS CIO and DHS DCIO Council.

3.2 Phase 2 – Evaluation

The DHS CSP evaluation team assesses the target organization, along with any component organizations under the defined direction of that organization utilizing the latest version of the DHS CSP ESM.

The evaluation determines if the assessed Component's effectiveness meets the standard established in the DHS Cybersecurity Services ESM. Evaluation activities verify cybersecurity services are satisfactorily provided within the scope of the assessed Component's mission. Evaluation activities are dependent on the types of enclaves within the assessed Component's boundary.

The DHS CSP team will accomplish the following activities during the evaluation:

- A CSP assessment brief.
- Evaluate the effectiveness of the defense-in-depth methodology performed by the organization.
- Observe demonstrations of cybersecurity defense-in-depth attained by the assessed organization and boundary defense hierarchy above the assessed organization.
- Document, observe, and recommend effectiveness and best practices conducted on the organization's enclave/boundary.
- Provide out-brief to assessed Component organization's personnel and leadership.

3.3 Phase 3 – Reporting

The DHS CSP evaluation team prepares a CSP authorization recommendation for the assessed organization along with the assessment out-brief and, and if required, the first POA&M submission provided from the assessed organization. The CSP authorization recommendation is submitted to the DHS CIO 45 days post out-brief.

The CSP authorization recommendation letter provides an overall assessment of cybersecurity service capability and includes actions recommended to refine cybersecurity service delivery. The assessment out-brief contains DHS Cybersecurity Services ESM results consisting of observations of processes gathered during the evaluation along with identified deficiencies and recommendations. The evaluation out-brief includes both commendable actions, and any weaknesses identified in mission capabilities, practices, and procedures.

The DHS CSP reviews assessment results and first POA&M submission (if required), due within 30 days after organization receives final results, to make an appropriate authorization recommendation to the DHS CSP AO. If the DHS CSP evaluators determines the assessed organization complies with the requirements as defined by the DHS Cybersecurity Services ESM, they issue a letter of recommendation to the DHS CSP AO. The letter will include a recommendation to authorize all cybersecurity services, which met or exceeded the requirement. The DHS CSP evaluator may also make supplemental recommendations to the assessed organization for process improvements.

If the DHS CSP evaluator concludes the assessed organization has not met the requirements defined by the DHS Cybersecurity Services ESM, the authorization letter will include a recommendation to deny authorization.

Plans of Action and Milestones (POA&Ms) created in response to assessment results should follow all requirements for FISMA system POA&Ms as outlined 4300A, Attachment H with one key exception; CSP POA&Ms should have a completion date within 180 days, in order to comply with the timeline for retesting. This means that POA&Ms should identify the weakness being addressed, a reasonable number of milestones required for completion (at least two), objective measures to determine the completion of those milestones, and the scheduled completion dates.

The DHS CSP AO will review the authorization package and make the final decision for the CSP authorization to provide cybersecurity services for unclassified systems.

Based upon the review of the evaluation package from the DHS CSP evaluator, the DHS CSP AO will grant authorization through an Authorization Letter with conditions, as appropriate.

Authorizations are typically granted for terms of at least three (3) years but can be changed at the discretion of the DHS CSP AO.

The DHS CSP AO will approve an ATO to the assessed organization achieving the requirements defined in the DHS Cybersecurity Services ESM. The final authorization decision is issued to the assessed organization by the DHS CSP AO. The decision will contain all recommendations by the evaluator(s), the DHS CSP ATO, and any supporting documentation.

4.0 CSP SOC METRIC MATURITY LEVELS

The CSP introduces a comprehensive capability and service maturity model. The model defines five Maturity Levels (MLs), ML0 through ML4, that apply across all service areas. Each of the five defined MLs is further designated by a name, for example, "ML1: Performed". There are four aspects of the MLs that are important to understand for correctly applying the model:

- The MLs apply independently to each cybersecurity function or metric. As a result, a service provider may receive different ML ratings for different functions and not an overall or aggregated ML assessment.
- The MLs are cumulative within each cybersecurity function. To achieve an ML in a given metric, the evaluation criteria at that level and all preceding level(s) must be fully completed.
- Striving to achieve the highest ML in all metrics may not be optimal for all SOCs. However, thresholds are established for each metric which must be achieved at a minimum to receive authorization for that function.
- Some metrics have multiple criteria at the same ML. In metrics such as this all criteria for a given ML must be met to achieve that level.
- Where cybersecurity services are provided by multiple organizations, the lowest observed maturity will be noted/reported with a full description of the affected scope of IT assets to which that level of maturity is observed.

The Maturity Levels for the Identify, Protect, Detect, Respond and Recover service area metrics are categorized as follows:

Maturity Level	Rating	
ML0	Incomplete	Functions are either not performed or partially performed
ML1	Performed	Basic essential, mandated, and regulatory functions are performed
ML2	Advanced	Advanced functions are performed to provide a tailored service based on Subscriber(s) operational and/or mission requirements
ML3	Optimized	Process and capability improvement program has been implemented to track deficiencies and integrate lessons learned to continually driveoperational improvement
ML4	Innovative	Helping shape the integrated cyber mission space through collaboration with DHS and/or Non-DHS organizations

Table 1: CSP Maturity Levels

5.0 DHS CSP SOC METRICS

Metrics represent the specific National Institute of Standards and Technology (NIST) CSF cybersecurity functions required by DHS. DHS Component Chief Information Officers (CIO) and Chief Information Security Officers (CISO) must ensure all cybersecurity functions are performed for their IT Information Systems; however, they may elect to receive (i.e., become Subscribers of) these services from DHS organizations authorized to provide them or provide the services for themselves. These Providers may further elect to provide any of the services and/or functions identified by the metrics.

Each metric is numbered for reference and categorized by Service Activity. A Maturity Level Threshold is established for each metric and serves as the baseline for performance of that function. DHS SOCs will be evaluated through the Cybersecurity Service Evaluation Process. This process ensures that SOCs are performing all required services as noted in the Evaluation Criteria of each metric to receive and maintain authorization to continue providing those cybersecurity services to DHS Components. DHS Component organizations who subscribe to cybersecurity services from an authorized Provider must have those services validated through the Cybersecurity Service Evaluation Process. These Subscribers may expect to receive services in accordance with the Validation Criteria noted in each metric.

Assessment Artifacts are examples of documents, communications, cybersecurity tools, and other evidence that cybersecurity services are being performed. This list of artifacts is intended to be fluid to allow for changes as new or better examples evolve or technology advances.

5.1 NIST Cybersecurity Framework (CSF)

The formal evaluation is organized along the five major service areas of the NIST Cybersecurity Framework (CSF):

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome metrics within this function include Cyber Risk Assessment (CRM).

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome metrics within this function include: Vulnerability Assessment and Analysis (VAA), Vulnerability Management (VM), and Malware Protection (MP).

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome metrics within this function include: Information Security Continuous Monitoring (ISCM), Insider Threat; Warning Intelligence, and Attack Sensing and Warning (AS&W).

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The Respond Function supports the ability to contain the impact of a potential cybersecurity event. An example of outcome metrics within this function includes Cyber Incident Handling.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome metrics within this function include Program Management, Personnel, Security Administration, and Service Provider Information Systems.

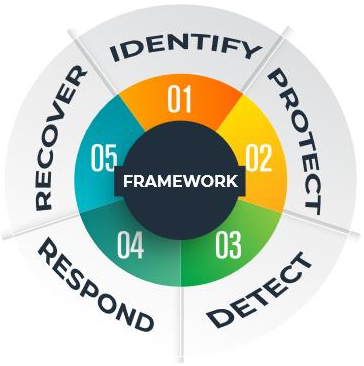

Figure 2: NIST CSF Framework

5.2 CSP SOC Metrics Details

Components/organizations are assessed using the Evaluator Scoring Metrics (ESM), a set of 40 metrics broken down into five (5) functions, covering 13 Process Areas, based on the NIST Cybersecurity Framework (CSF). The DHS ESM borrows heavily from the DoD's established Cyber Security Service Provider (CSSP) Program and was adapted to DHS policy by the CISO Council.

Each service area consists of various activities the SOC is responsible for providing to subscribers. For example, activities within the Protect service area include Vulnerability Assessment and Analysis (VAA), Vulnerability Management (VM), Malware Protection (MP), and Recoverability. Each activity consists of multiple metrics that are organized to determine the maturity of cybersecurity operations and are assessed based on evaluation criteria deemed crucial for its successful implementation.

5.3 Evaluation/Testing Methods

Cybersecurity service evaluators assess the performance of the metrics through four basic methods:

1. Examine artifacts – review policies, procedures, tools, capabilities, and other evidence of service activity.
2. Interview personnel – receive briefings and speak with those who perform or are responsible for service delivery.
3. Observe demonstration –observe cybersecurity operations and ask questions to gain a better understanding of the operations environment.
4. Performance metric – those functions that are candidates to be tested for successful performance as part of the Cybersecurity Service Provider Performance Evaluation Program.

6.0 DHS CSP ACCREDITATION LEVELS

Under the DHS CSP Program, each cybersecurity program within DHS will be inspected to determine their cybersecurity services capability maturity level.

Those entities that meet the minimum standard as defined by the DHS CSP Program will be deemed an accredited Cybersecurity Services program.

Entities that exceed the minimum standard as defined by the program will be accredited as a Center of Excellence (COE). The entity is then eligible to provide cybersecurity service offerings to other DHS Components, known as subscribers.

Term	Definition
Accredited	In the context of this program, an entity that meets the DHS CISO Council approved minimum set of criteria for having Cybersecurity Services capabilities. **As Accredited, the entity provides basic cybersecurity services to its organization only.**
Center of Excellence (COE)	An accredited DHS entity that meets the DHS CISO Council approved maturity criteria as specified by the DHS CSP Program, including providing cybersecurity capabilities at a level of maturity that demonstrates the use of best practices and enhances the efficacy of security operations. **A DHS COE that is accredited to provide cybersecurity services to other organizations within DHS in accordance with applicable standards and guidance as defined by the DHS CSP Program.** DHS CSPs will develop and maintain a service catalog that defines their authorized cybersecurity services offerings and the terms of agreements between the provider and subscriber.

*Table 2: **DHS Accreditation Levels***

7.0 CSP NOC ASSESSMENT FRAMEWORK

The CSP Program was expanded in FY 21 to include NOC assessments. NOC Metrics or Indicators were developed and designed to standardize 10 network processes from across four ITILv3 service lifecycles:

- Network Design
- Network Service Transition
- Network Service Operations
- Continual Service Improvement

In order to evaluate components against the NOC framework, the DHS team in coordination with ICE developed the NOC Evaluator Scoring Metrics (ESM). The framework based on Cybersecurity Service Program (CSP) NOC metrics developed utilizing the above ITIL processes and was coordinated between the DHS HQ ITOPS Directorate and the Office of the DHS CISO.

To accompany the NOC ESM, the CSP PMO developed a tool for DHS and its Components to conduct self and third-party assessments for Network Operation Centers (NOCs):

- The assessment criteria standardize NOC services for Component IT systems, as well as IT Information Systems of other Components within DHS.
- Each metric has a max score of 10, divided evenly among the applicable Measures of Performance (MOPs).
- Each measure may be C - Compliant, NC - Non-compliant, I - Inherited, or NA - Not Applicable.
- NAs are not counted towards scoring and inherited measures are treated as compliant for scoring purposes.
- Measures of Effectiveness (MOEs) are tracked for informational purposes only until further notice.
- Figure 3 below shows the grading rubric:

Legend:	
Metric	Total
< 7	< 70%
>=7 and < 8	>=70% and < 80%
>= 8	>= 80%

Figure 3: NOC Grading Rubric

- Component organizations that achieve a total score of 80% or above will be considered a NOC COE and can provide services to other organizations as described in Section 2.0 DHS CSP Accreditation Levels.
- Component organizations that achieve a total score between 70% and 80% will receive an accreditation that will allow them to provide services to their component only as described in Section 2.0 DHS CSP Accreditation Levels.
- Component NOCs receiving these designations will be inspected every three (3) years and will be assessed against all currently AO approved CSP NOC Metrics each time. Additionally, all Component Subscribers (those purchasing services from Accredited COEs) will also be assessed every three (3) years against all metrics to ensure the services received are meeting the required Maturity Levels.
- Components who fail to achieve a score of 70% or above must purchase services from a NOC COE.

8.0 STAKEHOLDERS AND RESPONSIBILITIES

8.1 DHS CSP Program Owner and CSP Authorizing Official (AO)

The DHS CIO has assumed the role of the DHS CSP Program Owner and CSP Authorizing Official (AO).

Responsibility(s):

- Assumes the role of DHS CSP Authorizing Official (AO) for all DHS Cybersecurity Service Providers Programs
- Unless formally delegated, highest-ranking agency official with overall responsibility for the implementation and management of the DHS CSP Program

- Resolves disagreements involving the cybersecurity assessment team and DHS entity assessed. which are not resolved by the DHS DCIO Council
- For entities that fail accreditation and any subsequent re-evaluation, the DHS CSP Program AO will determine the deadline by which the failed entity will be required to purchase cybersecurity services from a DHS CSP

8.2 DHS DCIO & DHS DCIO Council

Responsibilities:

- Provides strategic direction to the DHS CSP Program on behalf of the DHS CIO.
- As submitted by the DHS CSP PMO, the DHS DCIO approves all DHS CSP programmatic. documentation, i.e., program charter, metrics, target maturity levels, etc.
- Annually, at minimum, DHS DCIO approves DHS CSP Evaluator Scoring Metrics (ESM), as recommended by the DHS CSP Steering Committee.
- Monitors changes in DHS assessed entity accreditation and CSP certification status.

8.3 DHS CISO & DHS CISO Council

Responsibilities:

- In addition to DHS CISO Council responsibilities associated with the CSP Program, provides timely arbitration when decisions are not resolved by the DHS CISO Council specific to or impacting the DHS CSP Program.
- *Important*: DHS CISO Council, unless specifically requested in writing by the DHS CISO or CSP AO, on a case-by-case basis, does not receive details of any assessed entity scoring, etc. It only receives the summary of recommendation(s) in order to maintain the confidentiality of results and encourage open communication with the assessment team.
- Monitors CSP program-related POA&Ms for issues.
- Monitors CSP Steering Committee for changes in dates or impact aspects to POA&Ms and coordinates approval with the AO or designee.

8.4 DHS CSP Steering Committee

The DHS Steering Committee will be made up of one member per Component. The steering committee member should hold the title of Cybersecurity Operations Manager/SOC Chief and must be approved by the respective Component CISO.

Responsibilities:

- Provides cybersecurity technical, analytical, and coordination support to DHS Components, Federal Partners, and supporting CSPs conducting missions throughout DHS information systems and enclaves.
- Coordinates relevant cybersecurity issues and requirements between the DHS HQ/Component-level organizations directing and managing network operations and cybersecurity activities and supporting CSP(s) for in-scope information system.
- Serves as technical advisory committee to the DHS CSP PMO and DHS CISO Council for DHS-wide capability requirements are incorporated into the DHS CSP ESM as required.
- Verifies those operational requirements are included in the development of the DHS CSP ESM.

- Provides experienced technical members to advise the CSP PMO on developing technical elements of the DHS CSP ESM.

8.5 DHS CSP Federal Program Manager

Responsibilities:

- Operates from the DHS HQ CISO Directorate, within the DHS Agency OCIO Office.
- Will be an independent group of the CISO Directorate to remain neutral from any DHS HQ operations or cybersecurity services division or branch and will report directly to the agency CISO or higher.
- Federal Program Manager for the DHS CSP Program and DHS CSP PMO
- Provides Strategic direction and recommendations for the DHS CSP Program
- Primary and Accountable Federal Lead for all DHS CSP Assessments and operational aspects of the program.
- Provides operational direction, decisions, and guidance for all DHS CSP Assessments.
- Consults and formally meets with the DHS CISO Council monthly.
- Establishes and monitors DHS CSP Assessment Schedules.
- NLT end of Q1 of the Fiscal Year, presents and receives approval for the published CSP Assessment Schedule from the DHS CSP Steering Committee.
- Subsequent significant changes to the schedules should be presented to the DHS Steering Council for comment before any updated publication.
- In consultation and concurrence with the DHS CSP Steering Committee, approves all recommendations for DHS CSP accreditations prior to submission to the DHS CSP AO.
- Produces, for the DHS CISO Council and DHS CSP CISO Council, a monthly status report and/or briefing, to include, at minimum:
- Executive, action-oriented and Program-level (programmatic) status highlighting any program or operational risks or issues for DHS CISO Council to action or for awareness
- Summary consolidated list of POA&Ms being tracked (open/closed) by the DHS CSP PMO regarding CSP accreditation.
- DHS CSP Assessment Schedules and Status
- In consultation and concurrence with the DHS CSP Steering Committee, provides annual documented recommendations to the DHS CISO Council regarding the DHS CSP Program's:
    - Target Maturity Levels
    - Enterprise Security Metrics
    - Program processes, procedures, documentation and/or governance

8.6 CSP Program Management Office (PMO)

Responsibilities:

- Develops and maintains all program charters for the DHS CSP program and supporting sub-groups, committees, etc.
- Manages day-to-day activities of the DHS CSP Program.
- Responsible for the oversight of the DHS CSP Assessments.

Performs evaluations to assess the effectiveness and performance of DHS HQ/Component-level organizations directing and managing network operations and cybersecurity activities and supporting CSP(s) for unclassified information systems.

- Develops and revises DHS Cybersecurity Services ESM as the criteria for cybersecurity authorization assessments based on the defined activities within DHS Sensitive Systems Policy Directive 4300A and this attachment.
- Develops, maintains, and enhances a formal information system DHS cybersecurity service assessment program that includes:
    - Mission-based cyber threat inspections to validate the DHS HQ/Component's ability to conduct its mission and protect its assets and capabilities in accordance with DHS requirements.
    - Verification and assessment of DHS HQ/Component-wide coverage for all required cybersecurity activities and recommendations for remediation of cited shortfalls.
    - A cybersecurity service validation process to ensure the execution and delivery of cybersecurity services to a DHS subscriber by an authorized DHS provider are conducted.
- Provides to the DHS CSP AO, for the purposes of including their consideration as components of CSP assessments, with summaries of findings from each assessed entity's CSP assessment.
- Prepares DHS evaluation documents with a recommendation to authorize the service provider to offer cybersecurity services for DHS systems.
- Maintains meeting minutes for all relevant meetings and committees and available in a centralized location – available at minimum to the DHS CSP Steering Committee members and DHS CISO Council.
- Maintains all program documentation and appropriate reporting in an accessed controlled, secure, and centralized location – available at minimum to the DHS CSP Steering Committee members and DHS CISO Council.
- Tracks the status of all remediations, ATOs, and services offered and provided. Metrics tracked will include the number of open and overdue POA&Ms for each Component, tracked by standard and core metrics.
- Tracks the ATO status and expiration date for all accredited components. The services being provided by components, and the components receiving those services.
- Schedules and coordinates with components for preassessment, assessment, and post-assessment activities.

8.7 CSP Assessors/Assessment Team

The CSP PMO will maintain a dedicated team for assessment support of qualified assessors and project management professionals to conduct assessments and support PMO requirements. The CSP PMO will be responsible for providing appropriate training and development for designated assessors. This will ensure a level of neutrality for all assessments and ensure assessors are well-trained, familiar with DHS policy, procedures, and tools.

Responsibilities:

- Performs CSP Assessments on Component entities utilizing the appropriate ESM.
- Reviews Component self-assessment and artifacts.
- Assessors can participate in the DHS CSP Steering Committee as observers or presenters.

The following general requirements are recommended for this role:

- Full understanding of relevant reference policies as identified in this document, especially DHS 4300 series.
- Background in DHS agency-wide and/or component-specific program and project management methodologies.
- Thorough understanding of the DHS CSP ESM (metrics).
- Direct Experience with Cyber Security Operations Centers specifically, as well as cybersecurity services program as a whole.
- Significant experience in standards-based assessments.
- Understanding the scope and unique requirements a fully operating cybersecurity services program.
- Additionally, and as an example, assessment teams will be asked to recommend appropriate and consistent remediation actions and artifacts if an approved measure/metric is not met.

8.8 Component Liaison

This role is required and assigned by the assessed entity ahead of any formal assessment by the DHS CSP. A senior Federal POC will be formally assigned by the assessed entity to manage and coordinate all aspects of the DHS CSP Assessment for their respective Component.

Responsibilities:

- This individual will be the focal point and interface for the remote/on-site DHS CSP program assessment team lead.
- Coordinate the schedule with the CSP PMO and entity personnel participating in interviews/walkthroughs.
- Ability to discuss CSP roadblocks/issues directly with the assessed entity's CISO or Deputy CISO (or relevant peer) when appropriate.
- DHS CSP PMO will notify the component CISO (or appropriate other) three (3) months prior to any DHS CSP Assessment to receive this Liaison's contact information.
- Provide access to all requested/required DHS Component capabilities, assets, and data to DHS CSP inspection and assessment team(s).
- If utilizing external government / commercial services, the DHS Assessed Entity is responsible to coordinate access for DHS CSP inspection and assessment team(s).

9.0 ACRONYM LIST

AO- Authorizing Official
ATO- Authority to Operate
CIO- Chief Information Officer
CISO- Chief Information Security Officer
CMM- Cybersecurity Maturity Model
COE- Center of Excellence
CRM- Cyber Risk Assessment
CSF- Cyber Security Framework (NIST)
CSP- Cybersecurity Service Provider
CSSP- Cyber Security Service Provider
DHS- Department of Homeland Security
EO- Executive Order
ESM- Evaluator Scoring Metric
FISMA- Federal Information Security Management Act
ISCM- Information Security Continuous Monitoring
ML-Maturity Level
MOE- Measures of Effectiveness
MOP- Measures of Performance
NC- Non-compliant
NIST- National Institute of Standards and Technology
NOC- Network Operations Center
OCIO- Office of the Chief Information Officer
OCISO- Office of the Chief Information Security Officer
PMO- Project Management Office
POAM-Plans of Actions and Milestones
SME-Subject Matter Expert
SOC- Security Operations Center
VAA- Vulnerability Assessment and Analysis
VM- Vulnerability Management