Department of Homeland Security (DHS)
Science & Technology Directorate (S&T)
Office of University Programs (OUP)

DHS University Programs Portal Project

IT Requirements Document

January 28, 2020

TABLE OF CONTENTS

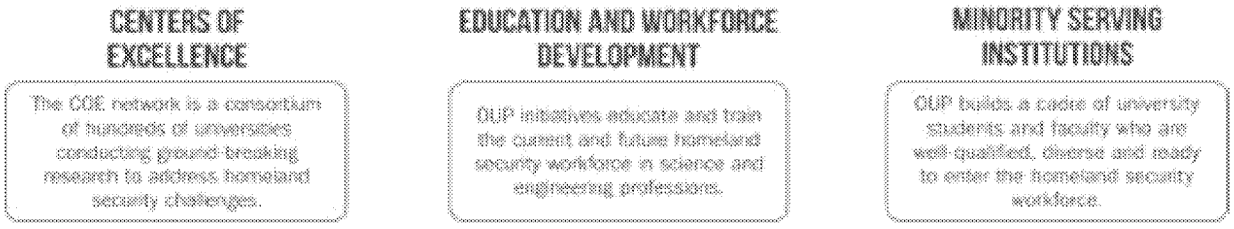
1 Introduction

The Homeland Security Act of 2002 charges the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office of University Programs (OUP) with establishing "a coordinated, university-based system to enhance the Nation's homeland security, supporting United States leadership in science and technology and conducting merit review of research and development projects … and the dissemination of research conducted or sponsored by the Department."

This includes:

- Generating, advancing, and disseminating knowledge, prototypes, and technologies in support of DHS Component identified operational and strategic challenges;
- Building a stable community of homeland security researchers and educators at U.S. colleges and universities capable of providing DHS with novel insights and approaches in diverse scientific domains;
- Strengthening the U.S. scientific leadership in homeland security research and education; and
- Developing a permanent homeland security science and engineering workforce.

DHS S&T OUP meets these objectives through the DHS Centers of Excellence (COEs) and Minority Serving Institutions (MSI) programs, which constitute a complex and broad portfolio of scientific investments focused on the investigation, experimentation, and evaluation of emerging science and technology in response to DHS Component needs.



OUP requires an online portal to facilitate information sharing between DHS, other federal agencies, COEs, MSI grant recipients, public- and private- sector partner networks, and the public. OUP commissioned the drafting of a Visioning Document to convey the purpose and high-level capabilities desired in a collaborative portal solution. Based on OUP's Vision Document, two separate detailed requirements documents were created; one to detail the functional capability requirements necessary for the features and functions of the system to satisfy OUP's operational needs and the other to detail the Information Technology (IT) requirements necessary for the solution to function within the intended, government-owned, hosting environment. This document details the IT requirements for the OUP Portal.

2 Scope of Engagement and Assumptions

The following define the scope of engagement and expected responsibility division between the DHS S&T Office of Enterprise Services (OES), Office of the Chief Information Officer (OCIO) and OUP for the design, build, test, launch and maintenance of the OUP Portal.

2.1 Scope of S&T OES CIO Engagement with OUP

S&T CIO will:

2.1.1 Establish a Cloud tenant on the S&T Gov Cloud Environment.

2.1.1.1 Establish the tenant on Amazon AWS or Microsoft Azure cloud platform.

2.1.1.2 Provide network configuration to the cloud, including V-LAN.

2.1.1.3 Submit DNS requirements, Firewall rules, and Configuration template.

2.1.2 Provide Security Services

2.1.2.1 Conduct vulnerability assessment and penetration testing customized to the system function and technical requirements.

2.1.2.2 Ensure FIPS 140-2 validation.

2.1.2.3 Provide ISSO Services.

2.1.2.4 Provide hardening guidance and STIG Ver 1, Rel 2.

2.1.3 Provide O&M Services at the infrastructure layer

2.1.3.1 Provide O&M support in the cloud.

2.2 Scope of OUP Engagement with S&T OES CIO

OUP will:

2.2.1 Provide contractor support for the OUP application in the cloud.

2.2.2 Request DHS suitability for contract support.

2.2.3 Provide required application software upgrades and patches.

2.2.4 Provide technical specifications for the cloud.

2.2.5 Provide URL if required, IP and Port number for license validation.

2.2.6 Comply with forensic requirement (access identification, authentication, and authorization; storage and retention; etc.).

2.2.7 Provide a PM to coordinate with S&T CIO regarding project updates.

2.3 Assumptions

The design, test, build and launch of the OUP Portal solution using these requirements makes the following assumptions:

2.3.1 OUP Proof-of-concept Data Evaluation will reside on DHS S&T's certified AWS or Azure cloud

2.3.2 IT Security Compliance will be provided with the following activities: patch management, vulnerability scanning, OS Hardening, change management, configuration management, review board, and any approval processes.

2.3.3 All system design and changes shall be reviewed and approved by S&T CIO Information Systems Security Officer (ISSO) under the oversight DHS S&T CIO Security Architect.

2.3.4 OUP will be responsible for workstation and the application administration and support.

2.3.5 All relevant DHS and Office of Management & Budget (OMB) IT directives and mandates shall be met for deployed solutions.

2.3.6 OUP shall submit a DHS S&T CIO Software Exception Requests (SER) and S&T Technical Reference Model (TRM) insertion requests, to expedite the listing of these products in the DHS Approved Products List (APL).

2.3.7 OUP Proof-of-concept Data Evaluation shall pass a vulnerability scan with low risk results.

2.3.8 OUP shall label documentation as Unclassified//Official Use Only.

2.3.9 All OUP Proof-of-concept Data Evaluation OS and Database configuration settings that cannot be applied to harden to the DHS hardening guidance, due to rendering the application inoperable, shall be documented with specific justification and submitted by the S&T ISSO to the DHS S&T Chief Information Security Officer (CISO) as a Waiver.

2.3.10 Anticipated Initial Operating Capability (IOC) 12-months from Phase II project start.

2.3.11 Anticipated Full Operating Capability (FOC) 6-months after achieving IOC.

2.3.12 Other potential IT deliverables from OUP will be implemented in a subsequent release under a separate Functional Requirements Document (FRD) and Project Cost Estimate.

2.3.13 All relevant DHS and Office of Management & Budget (OMB) IT directives/instructions and mandates will be followed during the course of this engagement. This includes but is not limited to DHS Sensitive Systems Policy Directive 4300A.

3 IT Requirements

The main drivers of the IT requirement the OUP's Portal solution are any potential limitations imposed by the hosting environment, constraints resulting end-users such as the system or software they must use or the networks or locations they must access the portal from, the information security/accreditation and privacy data related requirements mandated by DHS, system performance/availability metrics, and finally the certifications and/or training DHS mandates supporting contractors must have in order to work on the systems. The IT requirements that follow are grouped according each of these main requirement areas.

3.1 Environment Specific Requirements

OUP's original vision allowed for hosting at either a DHS managed datacenter or within a GovCloud environment. However, meetings with the Science and Technology (S&T) Office of the Chief Information Officer (OCIO) staff revealed that DHS datacenters are being phased out and GovCloud hosting is the only true long-term solution. For this reason, this IT requirements document reflects hosting in a GovCloud environment only. The currently allowed GovCloud environments include Amazon Web Service (AWS) West and Microsoft Azure Northern Virginia.

Utilizing the dhs.gov domain will require approval from the DHS OCIO. S&T OCIO will assist with the request, but the approval can take eight weeks. Once approval from use of the name is obtained from the DHS OCIO, the contractor shall work with S&T OCIO to procure the necessary server certificates for the public facing website. Certificate procurement will take approximately two weeks. Once procured, the OCIO will install the certificates on the OneNet BlueCoats. Certificate installation and testing will take approximately one month, resulting in an overall duration of 14 weeks from initial request for approval to having the certificate installed, tested, and availability for use.

3.1.1 The solution shall be hosted from either Amazon Web Services (AWS) Gov-West or Azure Northern Virginia.

3.1.2 The solution shall only use serverless functionality from either AWS or Azure that is available in the GovCloud. Features only available on the commercial side of either environment may not be proposed for use by the OUP Portal.

3.1.3 Functional requirements of the portal solution that cannot be satisfied using GovCloud serverless features may be satisfied by approved software/applications running on a virtualized server hosted in the GovCloud. Any server-based solutions must use either RedHat Linux version 7, Windows Server 2016, or Windows Server 2019.

3.1.4 The system shall be hosted within a single domain, ideally https://universityprograms.dhs.gov.

3.1.5 The contractor shall work with S&T OCIO to define all of the firewall rules necessary for the solution to work. There are technically no limitations to what can be configured.

3.1.6 The solution shall communicate with end user clients using no less than 2048 bit encrypted tunneling.

3.1.7 The solution shall support system to system data sharing efforts via REST protocol.

3.1.8 The solution provider shall provide detailed diagrams and documentation for all required ports and protocols.

3.1.9 The solution shall require SMS and Email notification be supported.

3.1.10 The solution shall function within a Network Address Translation (NAT) environment.

3.1.11 The solution shall be compatible with inline packet filtering or other inline network security measures.

3.2 Client (End User) Based Requirements

The following considerations with regard to the end-users' systems shall be taken into account when designing the Portal solution.

3.2.1 The solution shall be agnostic (Windows, Mac, Linux) to end user operating systems.

3.2.2 The solution shall support the latest versions of client browsers (ex: Chrome, Firefox, Safari, Edge/IE).

3.2.3 The solution shall support the following mobile platforms (Apple's iOS, and Google's Android).

3.2.4 The solution shall allow for DHS and non-DHS users alike.

3.2.5 The solution shall support users connecting from non-Government networks.

3.3 Security, Accreditation, and Data Privacy Requirements

The Portal solution will be required to obtain an Authority to Operate (ATO), a Privacy Impact Assessment (PIA), and a Systems of Records Notification (SORN) prior to portal build and launch. The requirements that follow detail the contractor's responsibilities in supporting the required accreditation processes.

If the Portal solution leverages virtual servers to host software/products that are not part of the GovCloud offering, those products will need to be approved for use by the S&T OCIO. If a product is not already listed as "Approved" in TRM, the contractor is able to submit a Software Exception Request (SER) in order to obtain approval to use a product/solution while it undergoes testing to verify that it is acceptable to use. A SER approval typically takes from one to three months depending on complexity of program in question. However, there is a risk involved due to the fact that an approved SER does not mean the solution will receive ultimate approval to operate within the OneNet environment. Therefore it is strongly recommended that all solutions considered be those currently listed as "Approved" in TRM.

3.3.1 The solution shall adhere to all requirements driven by DHS Authority to Operate (ATO) process.

3.3.2 The solution shall only use serverless functionality (PaaS) from either AWS or Azure that is available in the GovCloud. Features available only on the commercial-side of either environment shall not be proposed for use by the OUP Portal.

3.3.3 If using server-based applications, the solution shall not attempt to utilize any DHS restricted or banned technologies, as indicated by a Status equal to "Restricted" in TRM.

3.3.4 The System shall follow the DHS NIST FISMA Work-flow to set the necessary controls and conditions required to meet the communication, network, and compliance standards.

3.3.5 The solution shall be FISMA compliant.

3.3.5.1 The contractor shall patch known critical vulnerabilities within 30 days.

3.3.5.2 The contractor shall maintain the configuration baseline for the deployed solution and perform configuration management

activities in a manner that is consistent with OUP's change control policies, procedures, and processes.

3.3.5.3 The identity and access management solution shall provide Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 for non-privileged users.

3.3.5.4 The identity and access management solution shall provide Identity Assurance Level (IAL)4/Authenticator Assurance Level (AAL) 4 for privileged users.

3.3.5.5 The solution shall support the principles of least privilege and separation of user duties.

3.3.5.6 If the solution permits remote access, the contactor shall ensure that FIPS 140-2 validated cryptographic modules are implemented for its remote access connection method(s), remote access sessions time out after 15 minutes (or less), and that remote users' activities are logged and reviewed based on risk.

3.3.5.7 The solution shall ensure Federal Information Processing Standards (FIPS)-validated encryption of PII and other agency sensitive data both at rest and in transit.

3.3.5.8 The servers comprising the Portal solution shall be covered by an intrusion prevention system, where actions taken by the system are centrally visible at the enterprise level.

3.3.5.9 The servers comprising the Portal solution shall be covered by a software asset management capability centrally visible at the enterprise-level that is able to detect unauthorized software and alert appropriate security personnel.

3.3.6 The solution shall be DHS 4300A compliant.

3.3.7 The solution shall be FEDRAMP compliant.

3.3.8 The solution shall be NIST compliant.

3.3.9 The solution shall encrypt all data at rest and in transit to at least Advanced Encryption Standard 256 (AES 256).

3.3.10 The solution shall use a single authentication and authorization source across all components comprising the portal solution.

3.3.11 The solution shall support no less than 2046bit encryption for all https:// communications.

3.3.12 The solution shall audit and log all user and group activities both at the operating system level and within the application level.

3.3.13 The solution shall support access control levels that are defined by country-boundaries.

3.3.14 All code will need to pass through the S&T IA Compliance for acceptance prior to being applied to any DHS Area of Responsibility (AOR).

3.3.15 A Privacy Threshold Analysis is required to determine if PII is being collected and, if so, what types are collected and how is it being used.

3.3.16 The contractor shall be required to develop a Privacy Impact Assessment (PIA) and Systems of Records Notification (SORN) prior to portal build and launch.

3.4 System Availability Requirements

3.4.1 System availability shall meet or exceed 99.5% except during scheduled maintenance.

3.4.2 Scheduled maintenance impacting system availability shall be conducted outside of the hours 8:00AM – 8:00PM EST.

4 System Design and Compliance Requirements

4.1 Applicable to All DHS IT Systems

All IT systems (as defined by DHS Management Directive 0007.1) being planned, designed, developed, and maintained for the Department of Homeland Security, Science and Technology Directorate (DHS-S&T), its customers, and/or with DHS data, shall be:

4.1.1 In compliance with appropriate OMB Circulars, including but not limited to OMB Circulars A-11 and A-130 as implemented by the S&T CIO.

4.1.2 In compliance with federal regulations including but not limited to the E-Government Act (including Privacy Impact Assessment), Paperwork Reduction Act, Federal Information Security Management Act (FISMA), Section 508 of the Rehabilitation Act.

4.1.3 In compliance with DHS Management Directives including 0007.1, 4010.2, 1400, 4300.1 (and 4300A), 4900, and others as appropriate.

4.2 Homeland Security Enterprise Architecture (EA)

All IT systems (as defined by DHS Management Directive 0007.1) being planned, designed, developed, and maintained for the Department of Homeland Security, Science and Technology Directorate (DHS-S&T), its customers, and/or with DHS data, shall be:

4.2.1 All developed solutions and requirements shall be compliant with the HLS EA.

4.2.2 All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.

4.2.3 Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

4.2.4 Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.

4.2.5 Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. V480Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

4.2.6 Other guidance and best practices related to the Secure Coding Initiative and secure coding verification also apply.

5 Applicable Laws, Regulations, Policies and Publications

The following policies apply to the development, deployment, and operation of the OUP Portal. The key requirements associated with these policies are reflected in the IT Requirements defined in Section 2. The following are laws, regulations, and policies and related publications that pertain to this work effort. The contractor should be familiar with the guidance and requirements of each.

5.1 Public Laws and United States Code (U.S.C.)

- Public Law (P.L.) 107-347 Section III, Federal Information Security Management Act (FISMA) of 2002, 2002
- P.L. 107-305, Cyber Security Research and Development Act of 2002
- P.L. 96-456, Classified Information Procedures Act of 1980
- 5 U.S.C. 552, Freedom of Information Act; Public Information; Agency Rules, Opinions, Orders, Records, and Proceedings, 1967
- 5 U.S.C. 552a, Privacy Act; Records Maintained on Individuals, 1974
- 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices
- 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers
- 40 U.S.C. 1401 et seq., P.L. 104-106, Clinger Cohen Act of 1996 (Information Technology and Management Reform Act of 1996)
- 44 U.S.C. 3534, Federal Agency Responsibilities
- 44 U.S.C. 3535, Annual Independent Evaluation
- 44 U.S.C. 3537, Authorization of Appropriations
- 44 U.S.C. 3541, P.L. 107-296, Federal Information Security Management Act of 2002 (FISMA)
- 44 U.S.C. 3546, Federal Information Security Incident Center
- Government Paperwork Elimination Act (GPEA) http://www.whitehouse.gov/omb/fedreg/gpea2.htm

5.2 Office of Management and Budget (OMB) Circulars and Memoranda

- OMB Circular A130 http://www.whitehouse.gov/OMB/circulars/a130/a130.html
- OMB Policy Memorandum M-07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems.
- OMB Memorandum M-07-18, Ensuring New Acquisitions Include Common Security Configurations
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, 2000

5.3 Homeland Security Presidential Management Directives

- Homeland Security Presidential Directive HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, 2004 HSPD-20 National Continuity Policy
- DHS Management Directive (MD) 142-01 Information Collection Program (Paperwork Reduction Act 1995) 7/31/2007

- DHS MD 0007.1 Information Technology Integration and Management
- DHS MD 0475 Information Collection Program
- DHS MD 0550.1 Record Management
- DHS MD 0565 Personal Property Management Directive
- DHS MD 1120 Capitalization and Inventory of Personal Property
- DHS MD 1400 Investment Review Process
- DHS MD 3120.2 Employment of Non-Citizens
- DHS MD 4010.2 Section 508 Program Management Office & Electronic and Information Technology Accessibility
- DHS MD 4200.1 IT Capital Planning and Investment Control (CPIC) and Portfolio Management
- DHS MD 4300.1 Information Technology Systems Security
- DHS MD 4400.1 DHS Web (Internet, Intranet, and Extranet Information) and Information Systems
- DHS MD 4500.1 DHS E-Mail Usage
- DHS MD 4510 Domain Names
- DHS MD 4600.1 Personal Use of Government Office Equipment
- DHS MD 4800 Telecommunications Operations
- Attachment A: Frequently Asked Questions (FAQs)
- Attachment B: Nomination and Designation of Designated Agency Representative (DAR) for Telecommunications Services
- Attachment C: Designated Agency Representative (DAR) for Telecommunications Services Function Requirements
- DHS MD 4900 Individual Use and Operation of DHS Information Systems/ Computers
- DHS MD 8200.1 Information Quality
- DHS MD 11005 Suspending Access to DHS Facilities, Sensitive Information, and IT Systems
- DHS MD 11042.1 Safeguarding Sensitive But Unclassified (For Official Use Only) Information
- DHS MD 11056.1 Sensitive Security Information (SSI)
- DHS MD 11060.1 Operations Security Program
- DHS SELC (Systems Engineering Lifecycle) (Directive 102-01, Appendix B) Nov 2008

5.4 NIST Standards and Publications

National Institute of Standards and Technology (NIST), Special Publications (SP). The web site www.nist.gov contains the NIST publications.

- 800-18, Guide for Developing Security Plans for Information Technology Systems, 1998
- 800-23, Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products, 2000
- 800-26, Revised NIST SP 800-26 System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings, 2005
- 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, 2004
- 800-30, Risk Management Guide for Information Technology Systems, 2002
- 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, 2004
- 800-47, Security Guide for Interconnecting Information Technology Systems, 2002
- 800-53, Recommended Security Controls for Federal Information Systems, 2005
- 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories, 2004
- 800-61, Computer Security Incident Handling Guide, 2004
- 800-64, Security Considerations in the Information System Development Life Cycle, 2004
- 800-70, The NIST Security Configuration Checklists Program

5.5 FIPS Publications

- Federal Information Processing Standards Publications (FIPS PUBS). The web site http://www.itl.nist.gov/fipspubs/ contains FIPS publications.
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2003.

5.6 Other Information Technology Standards

- The contractor shall comply with Electronic and Information Technology Standards as specified on Web site http://www.section508.gov/index.cfm?FuseAction=Content&ID=3.
- Records management guidance for agencies implementing electronic signature technologies http://www.nara.gov/records/policy/gpea.html
- Electronic Signatures in Global and National Commerce Act (ESIGN) http://www.whitehouse.gov/omb/memoranda/m00-15.html