Logo

Description automatically generated

U.S. Department of State

Evolve

Attachment J-36

Sample Task Order for

Customer Support and Mobile Services

SOLICITATION  
19AQMM22R0029

**OCTOBER 2022**

Performance Work Statement

Table of Contents

[1.0 General 3](#_Toc106460300)

[2.0 Task Order Performance Requirements 8](#_Toc106460308)

[2.1 Task Area 1: Customer Support Services 8](#_Toc106460309)

[2.2 Task Area 2: Customer Endpoint Services 10](#_Toc106460310)

[2.3 Task Area 3: IT Service Management 24](#_Toc106460311)

[2.4 Task Area 4: Project and Surge Support 36](#_Toc106460312)

[2.5 Task Area 5 Special Projects and Subject Matter Expert Support 36](#_Toc106460313)

[2.6 Task Area 6: Cross-Functional Requirements 36](#_Toc106460314)

[3.0 Special Requirements/Instructions 46](#_Toc106460315)

[3.1 Standards (e.g., 5 FAM 600) 46](#_Toc106460316)

[3.2 Government-Furnished Equipment / Information 46](#_Toc106460317)

[3.3 Government-Data 46](#_Toc106460318)

[3.4 Place of Performance 46](#_Toc106460319)

[3.5 Standard Work Hours 46](#_Toc106460320)

[3.6 Facilities & Communication Tools 47](#_Toc106460321)

[3.7 Organizational Conflict of Interest (OCI) 48](#_Toc106460322)

[3.8 Associate Contractor Agreements 49](#_Toc106460323)

[3.9 Travel 50](#_Toc106460324)

[3.10 Other Direct Costs 50](#_Toc106460325)

[3.11 Funding 50](#_Toc106460326)

[3.12 Invoice Approval 50](#_Toc106460327)

[3.13 Earned Value Management System Requirements 50](#_Toc106460328)

[4.0 Task Order Management 50](#_Toc106460329)

[4.1 Key Personnel 51](#_Toc106460330)

[4.2 Transition 54](#_Toc106460331)

[4.3 Project Management Plan 55](#_Toc106460332)

[4.4 Meetings 55](#_Toc106460333)

[4.5 Measurements and Reporting 56](#_Toc106460334)

[4.6 Points of Contact 58](#_Toc106460335)

[4.7 Environmental and Energy Conservation Objectives 59](#_Toc106460336)

[5.0 Performance Requirements 59](#_Toc106460337)

[5.1 Quality Control and Quality Assurance 59](#_Toc106460338)

[5.2 Basic Performance Standards 59](#_Toc106460339)

1. List of Tables

Table 1. Customer Support and Mobile Services Task Areas 4

Table 2. Tools 5

Table 3. Mobile Device Program Profile 18

Table 4. Cross Functional Requirements 36

Table 5. Federal Information Processing Standards Publications 39

Table 6. National Institute of Standards and Technology Publications 40

Table 7. Office of Management and Budget Publications 40

Table 8. Security Policies 41

Table 9. Associate Contractors 49

Table 10. Task Order Key Personnel 51

1. Performance Work Statement
2. For
3. Customer Support and Mobile Services
4. General
   1. Introduction

This Performance Work Statement (or “PWS”) sets forth the roles and responsibilities of the Parties for Customer Support and Mobile services provided under the EVOLVE IDIQ contract as part of the Customer and End User Support Services Functional Category. Customer Support and Mobile Services are the services and activities, as further detailed in this PWS, required to deliver a wide range of services on demand to Department of State (DOS) and its partners.

* 1. Background

The Department of State (DOS) has a demonstrated need for supporting its personnel (government and contractor) in their use of information technology so that their work can be accomplished efficient and effectively.

The Bureau of Information Resource Management (IRM), led by the CIO, empowers the Department of State (from here on, “Department” or “DOS”) to achieve its foreign policy mission by providing modern, secure, and resilient information technology (IT) services. Rapid changes in technology are transforming how our diplomats advance U.S. foreign policy by altering the way we connect with others and communicate information. Our diplomats require powerful new technologies to advocate policy positions, promote awareness, and enhance transparency – that is where IRM comes in. IRM is seeking to award multiple performance-based Task Orders (TOs) to govern, manage, design, engineer, operate, maintain, improve, and secure the Department’s mission critical IT infrastructure and its associated programs.

IRM’s foremost objective is to foster innovative, effective, and interconnected diplomacy by constantly improving, modernizing, and refreshing tools and services. IRM is expanding the use of collaborative information development and refinement to provide end users with accurate and useful information – anytime, anywhere. IRM supports new IT solutions that provide access to collaborative tools and enables mobility, while simultaneously protecting our information and IT assets against evolving cyber threats and vulnerabilities.

One aspect of IRM’s mission is to manage the relationship between IRM and its customers to promote the development, use, and support of information technology to further foreign diplomacy and policy. IRM accomplishes this by providing the following via Information Technology Infrastructure Library (ITIL) framework-based processes:

* Quality, customer-centric Tier I service desk support providing a single point of contact for Department IT products and services worldwide
* Round the clock support to ensure technology resources are available for maximum utilization enabling customer missions in the U.S. as well as abroad.
* Tier II support to all IRM endpoint customers
* Mobile and remote access capabilities for the Department’s domestic customers and occasional international customers.
* The Enterprise Virtual Contact Center (EVCC) technology utilized by other service desks throughout the Department.
  1. Objectives

DOS is seeking an industry partner to provide Customer Support and Mobile Services under the Evolve IDIQ contract vehicle. The objective of this task order is to acquire expertise and skilled resources that will deliver these services to IRM’s customer base while maintaining or exceeding acceptable quality levels (AQL). The contractor shall focus on the customer experience (C/X) while delivering the services and executing the processes and practices detailed in this PWS.

DOS is seeking the contractor’s assistance to employ an efficient and effective IT Service Management framework for in scope services; provide and conduct a skilled IT Service Desk, provide anytime, anywhere support for customer endpoints with the goal of supporting customers wherever they are using a combination of on-site and remote support as appropriate. Scope

The contractor shall provide the full range of Customer Support and Mobile Services to meet the mission needs of the Department. This task order will provide enhanced service delivery and response times to support mission users, their end user devices, and services through a comprehensive and efficient approach for supporting the Department’s global footprint.

Customer Support services are those services that are mostly customer facing or further elaborate upon the IT Service Management processes and supporting processes and services outlined. Services include Tier 0, Tier I, and Tier II endpoint support in the NCR, Domestic and Overseas field office and remote locations, provide VIP support, after-hours support, release management, hardware and software deployments, IT moves, in addition to providing GFE management, incident analysis, problem analysis, classified (secret level) system support “CLASSNET”, user account support & directory service support, and classified and SBU print server, network scanner/digital sender service, file shares & performance and analytic tool support.

The contractor shall support the IT Service Desk that serves as the single point of contact between the IRM, service providers, and users and manages incidents, service requests, communication with the users.

The IT Service Desk provides Tier I support for all Department IT services, including:

* Registering and classifying received Incidents and undertaking an immediate effort in order to restore a failed IT service as quickly as possible.
* Transferring Incidents to Tier II expert technical support groups if not Tier I resolution can be achieved
* Processing Service Requests and keeping users informed about their Incidents' status at agreed intervals.

The IT Service Desk manages and coordinates Tier II support for Customer Endpoints, including:

* Assuming responsibility for Incidents which cannot be solved immediately at Tier I with the goal of providing more in-depth technical support to restore a failed IT Service as quickly as possible.
* Escalating to Tier II support if the incident cannot be resolved in accordance with documented service escalation periods.

The IT Service Desk manages and coordinates Tier III support for Customer Endpoints, escalating issues to the underpinning service provider, including original equipment manufacturer (OEM) vendor support.

The contractor shall also support the Enterprise Virtual Contact Center (EVCC) which provides Contact Center As A Service (CCAAS) for the IT Service Desk and other service desks throughout the Department.

The contract shall provide Customer Endpoint Support for end users. The scope includes:

* Support for provisioning, managing, operating and maintaining customer endpoints for the Department and delivering centralized support to end users.
* Support for customer endpoints includes devices such as client compute physical desktops, portable laptops, tablets, thin/zero client machines, peripherals (including monitors, pointer devices and attached personal printers) by individuals to perform work. Scope includes both directly connected endpoints as well as mobile endpoints such as laptops and tablets remotely connected through a VPN, web proxy, or other remote connection type. Support for mobile devices, such as mobile phones and associated voice, text and data services.
* Support for endpoints shall be provided to customers whether they are in the office, on the go, at a remote worksite in U.S. or abroad, at one of the IT Marts, at a home office or alternate work area. To accomplish flexible and comprehensive support, the contractor shall use a combination of methods such as over-the-phone, remote management tools, deskside assistance, IT Mart service, or in limited cases, in home support.

The scope of this task order includes the following task areas outlined in the table below.

1. Customer Support and Mobile Services by Geography

|  |  |  |  |
| --- | --- | --- | --- |
| **IT Service** | **Scope of Support by Geography** | | |
| **NCR** | **Domestic** | **Overseas** |
| All Department IT Services | Tier I | Tier I | Tier I |
| All IRM IT Services | Tier 0, I | Tier 0, I | Tier 0, I |
| Endpoint Devices: Desktops, desktops, portable laptops, tablets, thin/zero client machines, peripherals (including monitors, pointer devices and attached personal printers) | Tier 0, I, II, management of Tier III OEM vendor support | Tier 0, I, II, management of Tier III OEM vendor support | Tier 0, I |
| Endpoint Devices: Mobile Devices | Tier 0, I, II, management of Tier III OEM vendor support | Tier 0, I, II, management of Tier III OEM vendor support | Tier 0, I, II, management of Tier III OEM vendor support |

* 1. Tools, Applications, and Technology

The following tools, applications, and technology listed in Table 1.2 are currently utilized in support of Customer Support and Mobile Services. These tools are in use at the date of this PWS but are subject to change at eh Department’s discretion.

1. Tools

| Tools |
| --- |
| IT Service Management (ITSM) systems (the Department is transitioning from BMC Remedy to ServiceNow) |
| Integrated Logistics Management System – Acquisition (Ariba) and Hardware Asset Management (Altiris) |
| Global Financial Management Systems (GFMS) – Cost Data and Acquisitions Data (Momentum) |
| Information Assurance Authority to Operate Systems – A&A data on IT Systems (Xacta) |
| Managing State Projects for Information Technology (MSP-IT) – (O365’s Project and SharePoint) |
| IT Investment Portfolio Management System (iMatrix based on Oracle Primavera) |
| Budget & Planning Management Systems (BPMS, formally called IRM Financials) (ServiceNow) |
| Allotment Management System (AMS) (ServiceNow) |
| Software Asset Management System (SAM) (ServiceNow) |
| Vendor Insights/Management System (VMS) (ServiceNow/Apptio) |
| Office Funds Tracking System (OFTS) (ServiceNow) |
| Configuration Management Data Base (CMDB) – IT Assets System (ServiceNow) |
| Department-approved Collaboration tools (Microsoft Teams, Webex, Zoom) |
| Department-approved Data Management and Visualization tools (Splunk, PowerBI) |

* 1. Environmental Constraints

The contractor shall:

* Comply with Government technical direction.
* Ensure all documents and advisory assistance is in compliance with the Federal Acquisition Regulation (FAR), Department of State Acquisition Regulation (DOSAR), as well as other DOS standards, policies, procedures and guidelines and will comply with applicable international and country-specific laws, regulations and guidelines.
* Use the DOS Managing State Projects for Information Technology (MSP-IT)
* Demonstrate a high degree of experience at collaboration and coordination with Federal stakeholders and other Contractors.
* Not conduct themselves or convey information in a manner that will give the appearance the Contractor is a Government representative and/or is authorized to make decisions on behalf of the Government. The contractor is not authorized to perform inherently governmental tasks.
* Comply with all DOS guidelines, protect classified and sensitive information and maintain accountability of government furnished equipment.
* Comply with any policies, processes, reporting requirements, etc. issued by the IRM/BMP/ITA Contract Management Division which overseas and centrally manages all IRM IT Service contracts, and must copy IRM/BMP/ITA/CM on all cost, performance, and deliverable status, including any performance issues.
* Work collaboratively with other Evolve vendors.
* Be willing to adapt to a reorganization of the Government offices in the IRM Bureau, which provide contract oversight, to better align with a streamlined service delivery model.
  1. Contract Type

This is a performance-based task order that utilizes Labor Hour Contract Line Items (CLINs).

1. Task Order Performance Requirements

For all task areas described herein, the contractor shall:

* Apply and adapt ITILv4 or currently approved general management practices to deliver Customer Support and Mobile services as a holistic program.
* Assure the transitions into the task order in a manner that guarantees little or no service delivery degradation from the expiring contract for similar services.
* Ensure all work activities are performed in a timely and cost-effective manner while maintaining the highest quality of performance to achieve expected outcomes.
* Communicate with customers in a professional and timely manner ensuring SLAs are met or exceeded.
* Ensure communications are thorough, accurate, timely, and tailored to the audience.
* Translate technical information into clear, readable content for use by non-technical personnel.
* Ensure all deliverables are formatted IAW 5 FAH-1 “Correspondence Handbook” unless otherwise directed by the Government.
* Organize, conduct, and attend meetings as required.
* Develop and deliver timely, complete, and accurate meeting artifacts as required.
* Use Government Furnished tools for ticket logging & handling.
* Use Government Furnished tools to manage all tasks in the PWS.
* Create and maintain electronic dashboards for tasks/services/processes listed in this PWS. Update those dashboards as new services and technologies are introduced into the environment. These dashboards will align with other IRM dashboards when applicable.
* Use DOS designated repositories for all deliverables as required. 
  1. Task Area 1: Customer Support Services

The contractor shall provide IT Service Desk and related services to serve as the entry point and single point of contact for incident resolution and service requests. In addition to the IT Service Desk, these services include providing walk-up support via the IT Marts and providing Contact Center as a Service (CCaaS) via the Enterprise Virtual Contact Center (EVCC).

* + 1. IT Service Desk Support

The Service Desk is the single entry and delivery point for the provisioning of end user support. The Service Desk manages and coordinates the handling of incidents, problems, non-Service Catalog Requests, and Service Catalog Requests with end-users and IT groups for both unclassified and classified networks.

The contractor shall:

1. Provide global 24x7x365 helpdesk support through various inputs such as phone, email, chat and software generated with availability and capacity requirements as documented in the SLA to meet patterns of business activity.
2. Use Government Furnished tools for ticket logging & handling and stipulated Government provided call management/call handling performance tools-and-applications.
3. Log information necessary for ticket in accordance with Department guidelines, which currently include the following information at a minimum: contact info, incident/service request, location and any other pertinent information such as error message and full customer e-mails, etc. and provide the customer with the ticket number either verbally, systemically (via tools), and/or e-mail. Note that this minimum information may change at the Department’s discretion.
4. Utilize knowledge sources such as the KEDB, Knowledge Library, Knowledge System, etc. to provide information for first contact resolution.
5. Categorize and prioritize tickets using Government approved processes and standards.
6. Manage all service requests and incidents including tasks associated with those service requests and incidents.
7. Provide first contact resolution (FCR) IAW Government guidelines.
8. Escalate tickets to Tier II/III as necessary following escalation procedures/guidelines.
9. Update tickets and track the progress of those tickets in accordance with Department guidelines.
10. Communicate with the customers, stakeholders and other organization on ticket status, outages and other communications in accordance with Department guidelines.
11. Resolve tickets upon receipt of reasonable confirmation of incident or service request resolution and/or request fulfillment and reflect the confirmation in the respective ticket. IAW Government guidelines
12. Conduct customer satisfaction surveys in accordance with Department guidelines
13. Track, update and report customer contact handling measurements, metrics and compliance of those in accordance with Department guidelines.
14. Provide Tier 0 services via Knowledge Articles, videos, Chatbots, notifications via Department approved methods including cables, emails, notifications, syslist (MS Group), Teams or other collaboration mechanisms and websites.
15. Provide SharePoint administration for CCS sites.
    * 1. Walk-up Support (IT Mart)

Provide walk-up support at the Harry S. Truman Building (HST) and State Annex (SA) 15, 0800h-1700h eastern standard time.

The contractor shall:

1. Use Government Furnished Software for ticket logging & handling
2. Log information necessary for ticket to include: contact info, incident/service request, location and any other pertinent information such as (error message and full customer e-mails, etc.) and provide the customer with the ticket number either verbally, systemically (via tool), and/or e-mail.
3. Utilize knowledge sources such as the KEDB and Knowledge Library to provide information for first contact resolution.
4. Categorize and prioritize tickets using Government approved processes and standards.
5. Manage all service requests and incidents to include tasks associated with those under the purview of this PWS.
6. Provide first contact resolution (FCR) IAW Government guidelines.
7. Escalate tickets to appropriate Tier II/III support groups.
8. Communicate with customers in a professional and timely manner ensuring service level agreements are met or exceeded.
9. Create file share folders and forward access requests to file share owners for approval and or grant file share/share drive access requests.
10. Track and report IT Mart measurements, metrics and compliance.
    * 1. Enterprise Virtual Contact Center (EVCC)

The EVCC is a 24x7x365 virtual contact center that provides Contact Center as a Service (CCaaS) to IRM and other service desks throughout the Department (e.g. Diplomatic Security). EVCC allows IRM Service Desk Analysts (SDAs) to receive customer contacts from a location outside of a Department Call Center with DoS users requiring authentication to Department OpenNet.

The EVCC uses Automatic Number Identification (ANI) to record the source phone number for the SDA to call back to if the telephone call is disconnected and can also be integrated into with the Department ITSM tool (e.g. ServiceNow) to automatically locate an existing caller record. Phone calls are recorded for quality assurance and training purposes.

The Contractor shall:

1. Support and maintain the EVCC to provide Contact Center as a Service (CCaaS) to IRM and other service desks throughout the Department.
2. Support Service Desks with onsite and remote workers for normal operations and Continuity of Operations (COOP) during a potential shutdown, e.g., COVID-19, inclement weather, telework, etc.
3. Provide session-based services covering voice, video, chat, presence, conferencing, message, contextual collaboration, federation, and clients’ experiences on personal and Government-issued devices.
4. Provide CCaaS services to include: basic Voice over Internet Protocol (VoIP), Voice Messaging, Instant Message with Integrated Presence, Mobility support to various personal and Government-issued devices, and Collaboration including basic and advanced Audio and Web Conferencing.
5. Ensure that EVCC is accessible by Service Desk Analysts (SDAs) from any Department-connected location, to include telework.
6. Provide Tier III level support for the EVCC.
7. Incorporate improvements and additional capabilities into the EVCC as required.
   1. Task Area 2: Customer Endpoint Services
      1. National Capital Region (NCR) Endpoint Support

The Contractor shall:

1. Track and report NCR Endpoint support activities.
2. Provide support for Local Registration Authority (LRA) for limited Virginia (VA), Maryland (MD), and Domestic locations only.
3. Manage encryption certification provisioning including issuing and revoking PKI certificates.
4. Provide support for Share drive and file server support, to include granting access
5. Provide break fix release management support.
6. Image endpoints with the most current approved image.
7. Deploy patches and other upgrades to equipment provided by the Government.
   * + 1. Endpoint Support

Endpoint support includes hardware and software support to include break fix for adds, moves, changes, dispositions.

The contractor shall:

1. Troubleshoot, install, configure and dispose of endpoints and networked peripherals.
2. Update tickets with quality information required for trend analysis and ticket resolution.
3. Follow asset and configuration procedures and policies for equipment installation, replacement and disposition.
4. Follow change procedures and policies for equipment, installation, replacement and disposition.
   * + 1. Peripheral Support

The contractor shall:

1. Provide Network SBU and Classified printer break fix support
2. Provide Network SBU and Classified scanner & digital sender break fix support
3. Provide Network Multi-function Devices (MFDs)/Multi-function Printers/Copiers (MFPs) troubleshooting. Copiers/MFDs managed by A/GIS/GPS are not in-scope of this requirement.
4. Troubleshoot other endpoint connected peripherals.
   * + 1. Conference Room Support.

The contractor shall:

1. Provide Tier II on-site support to conference room SBU endpoints.
2. Provide rudimentary troubleshooting of conference room audiovisual (AV) equipment and escalate to Tier III as necessary.
3. Manage conference room Organizational Unit (OU).
4. Periodically validate conference room resources are functioning as required ensuring functionality as outlined in the SLA or work instructions to proactively address service delivery issues.
   * 1. NCR VIP Endpoint Support

VIP support is limited to the HST, nearby annexes and Rosslyn (Arlington, VA).

The Contractor shall:

1. Track and report VIP Endpoint support activities.
2. Provide VIP endpoint support IAW more stringent VIP support SLAs.
3. Provide LRA support manage encryption certification provisioning including issuing and revoking PKI certificates.
4. Provide support for Share drive and file server support, to include granting access
5. Provide endpoint security management.
6. Maintain current anti-virus definition files on DOS managed equipment.
7. Monitor vulnerabilities and apply security patches IAW IA, DS guidelines.
8. Coordinate activities with Release and Deployment Management.
   * + 1. NCR VIP Endpoint Release Management Support

The contractor shall:

1. Image endpoints with the most current approved image.
2. Deploy patches and other upgrades to equipment provided by the Government.
3. Provide Endpoint Support.
4. Endpoint hardware and software support to include break fix for adds, moves, changes, dispositions.
5. Troubleshooting, installation, configuration and disposition of endpoints and networked peripherals.
6. Use Government Furnished Software for ticket logging & handling.
7. Update tickets with quality information required for trend analysis and ticket resolution.
8. Follow asset and configuration procedures and policies for equipment installation, replacement and disposition.
9. Follow change procedures and policies for equipment, installation, replacement and disposition.
   * + 1. NCR VIP Endpoint Peripheral Support

The contractor shall:

1. Provide Network SBU and Classified printer break fix support
2. Provide Network SBU and Classified scanner & digital sender break fix support
3. Provide Network Multi-function Devices (MFDs)/Multi-function Printers/Copiers (MFPs) troubleshooting. Copiers/MFDs managed by A/GIS/GPS are not in-scope of this requirement.
4. Troubleshoot other endpoint connected peripherals.
   * 1. After-hours support

The contractor shall provide after-hours support for VIP tickets as well as critical/high tickets in the NCR. After-hours endpoint support is outside of business day, core hours 0600h to 1900h, eastern standard time.

The contractor shall:

1. Monitor DOS services and assets ensuring availability and take actions to maintain availability.
2. Manage and monitor software deployments after-hours and take corrective actions as necessary.
3. Ensure services and assets that are brought down during after-hours maintenance windows are brought up and/or rollback procedures are initiated prior to core hours.
4. Provide early life support for release packages and warm transfer to core support teams.
5. Report after-hours activities on the weekly operations report and MPSR.
6. When not addressing after-hours specific tasks, work other ticket queues such as manage user accounts tickets during periods of increased volume.
   * 1. Field Office Support

Support to DOS field offices for unclassified and classified services/systems/equipment.

The contractor shall:

1. Coordinate all logistics and schedules associated with on-site issues.
2. Report field office support activities.
3. Provide remote troubleshooting IAW service request, incident and change procedures.
4. Provide on-site support to include:
5. Endpoint and Peripheral Support.
6. Endpoint hardware and software support to include break fix for adds, moves, changes, dispositions.
7. Troubleshooting, installation, configuration and disposition of endpoints and networked peripherals.
8. Use Government Furnished tools for ticket logging & handling.
9. Update tickets with quality information required for trend analysis and ticket resolution.
10. Follow asset and configuration procedures and policies for equipment installation, replacement, and disposition.
11. Communicate with customers in a professional and timely manner ensuring service level agreements are met or exceeded.
12. Provide additional on-site support as required IAW service request, incident and change procedures collaborating with Washington D.C. based Office of Primary Responsibility (OPR) as necessary for the following services/equipment/software:

* Video Teleconferencing (VTC) Support
* Conference room support to include Smartboards, projectors, endpoints, etc.
* Provide support for Local Registration Authority (LRA).
* Manage encryption certification provisioning including issuing and revoking PKI certificates.
* Un-interrupted Power Supply (UPS).
* Network Equipment.
* Cabling.
* Laptops.
* Non-consolidated Endpoints.
* Applications.
* Cryptographic equipment, must maintain a Top Secret Clearance and follow all DOS Guidelines for handling and maintaining crypto equipment.
* Manage disposition of DOS assets.
  + 1. Overseas Endpoint Support

Provide Tier II support and escalation to Tier III for overseas endpoints that are centrally managed. These include remotely-managed, mobile endpoints that reside in IRM’s centrally-managed active directory structure.

1. Perform configuration management of remotely-managed devices. Remotely deploy patches and other upgrades to equipment provided by the Government.
2. Register, track, and escalate incidents and problems reported by overseas IT administrators with their users’ remotely-managed endpoint devices.
   * 1. Classified (Secret Level) System Support “CLASSNET”
        1. CLASSNET Virtual Desktop Server Support

Staff supporting the Classified Citrix environment must have either Citrix Certified Professional – Virtualization (CCP-V) or Citrix Certified Expert – Virtualization (CCE-V) certifications. At least one Citrix engineer with CCE-V certification must be onsite at all times during core business hours

The contractor shall:

1. Continuously monitor servers using both manual and automated methods to assess the daily operational health of all servers, services, and interfaces of the Classified Citrix environment.
2. Analyze logs, EdgeSite reports, and other diagnostic data to assess trends related to performance, scalability, and availability and make recommendations for longer term improvements to the Citrix environment.
3. Troubleshoot, support, and perform administration tasks, such as take servers offline, reboot servers, start services, etc. to maintain ongoing systems operations.
4. Develop, maintain, test, and support disaster preparedness, high availability and recovery procedures IAW IRM hosted server environment and identify gaps and other risks.
5. Apply security and vendor patches to ensure the environment has compliant software.
6. Update servers with the latest releases of DOS standard operating environment (SOE) applications (e.g., MS Office, SMART, Acrobat, etc.).
7. Plan, schedule, and perform system backups and data restoration to ensure critical data and server images are available near line if needed IAW IRM hosted server environment.
8. Configure, test, and install new applications approved for the classified network (e.g., Google Chrome, Google Earth, etc.).
9. Participate with other IRM and DOS organizations as needed to troubleshoot and resolve system problems affecting domestic classified network availability, performance, stability, security, or other issues that require remediation.
10. Resolve individual customer support tickets and other customer issues related to logons, application access, performance, profile corruption, etc.
11. Develop and maintain written procedures, manuals, guides, and other documents to ensure the Citrix environment is well maintained and remains highly available including Operations Manual, Design Documentation, Systems Security Plan, Concept of Operations, etc.
12. Perform configuration management to ensure system baselines are documented.
13. Follow change procedures and policies with the goal of no unscheduled outages/latent changes.
    * + 1. CLASSNET Citrix Client Support

The contractor shall:

1. Enhance and patch the client images as needed to ensure the middleware, operating system, and configuration include compliant software.
2. Assist endpoint support staff to troubleshoot problems related to client connectivity to the Citrix environment.
3. Modify new client images for existing or future hardware to ensure the Classified network clients meet DOS security requirements and support effective connectivity to the Citrix environment.
   * 1. Remote Access Services Support

The Contractor shall operate, maintain, and support the Department’s Sensitive But Unclassified, Remote Access Services. These services include but are not limited to virtual desktop access (currently using a Citrix platform).

* + 1. Classified and SBU Print Server, Network Scanner/Digital Sender Service, File Shares & DOS Tools Management Services

The Contractor shall:

1. Follow all change, release and deployment processes.
2. Continuously monitor assigned servers using both manual and automated methods to assess the daily operational health of all servers, services, and interfaces.
3. Analyze logs, reports, and other diagnostic data to assess trends related to performance, scalability, and availability and make recommendations for longer term improvements to print server and scanner service.
4. Troubleshoot, support, and perform administration tasks, such as take servers offline, reboot servers, start services, etc. to maintain ongoing systems operations.
5. Develop, maintain, test, and support disaster preparedness, high availability and recovery procedures IAW IRM hosted server environment.
6. Apply security and vendor patches to ensure the environment has compliant software.
7. Update servers with the latest releases of DOS SOE.
8. Plan, schedule, and perform system backups and data restoration to ensure critical data and server images are available near line if needed IAW IRM hosted server environment and identify gaps and other risks.
9. Manage print server and network scanner resources ensuring availability and capacity of the service.
10. Use Government Furnished tools for ticket logging & handling.
11. Update tickets with quality information required for trend analysis and ticket resolution.
12. Participate with other IRM organizations as needed to troubleshoot and resolve system problems.
13. Develop and maintain written procedures, manuals, guides, and other documents to ensure the printer/scanner service is well maintained and remains highly available including Operations Manual, Design Documentation, Systems Security Plan, Concept of Operations, etc.
14. Perform configuration management to ensure system baselines are documented.
15. Follow change procedures and policies with the goal of no unscheduled outages/latent changes.
16. Report on printer/scanner support activities at a minimum at the MPSR.
17. Adhere to and support Task 4 activities concerning print server & network scanner/digital sender management.
18. Manage and maintain tools ensuring availability and fitness for use to include “Quick Check” a knowledge management tool and “Quick Scan” an AD tool.
19. At some unknown time during the performance of this task order these tools may be transitioned to a new platform at which time the level of effort will be changed and a changed order maybe executed.
20. Establish a proactive printer, MFD and scanner monitoring program that focuses on the customer experience not merely on back-office resource availability. KPIs shall be customer-centric.
21. Manage required software license for services under this task such as digital sender licenses.
    * 1. Mobile Services

The contractor shall provide mobile services using industry best practices and departmental guidelines to optimally operate and maintain the services in scope, and to provide engineering services. The system within which MRA conducts its business is called the MRA/MO Service Management System (SMS) and is described in the MRA/MO Service Management System Program Plan and follows the most recent publication, currently the BS ISO/IEC 20000-1:2011 Standard Publication.

Task area scope includes: Domestic Mobile Services, International Mobile Services, Mobile Engineering, Remote Access Services, Mobile Engineering, and Customer Operations Support Services. All task must be performed according to the NIST-aligned Mobile Minimum Technical Security Requirements found in the Appendix.

* + - 1. Domestic Mobile Services

The Contractor shall manage voice, text and data services (“Mobile Services”) domestically on a 24x7x365 schedule, to include procurement of services and service enabling devices. In addition to voice, text, and data services, the contractor shall provide additional domestic mobile services.

The contractor shall:

1. Perform fulfillment and return services for mobile devices
2. Provide Invoice Reporting services, including:
   1. Invoice reporting available on the contractor website
   2. Maintaining detailed logs and transactional records for auditing purposes
3. Provide Service Ordering services, including:
4. Ordering and disconnection of voice, text and data services
5. Web-based self-service tool for ordering devices and service
6. Maintaining a customer-facing catalog of devices and services plans
7. Provide Device Ordering services:
8. Support ordering of new and replacement devices
9. Have established agreements and providing considerable savings through volume discounts with industry-leading mobile device manufacturers and cellular service providers
10. Leverage the buying power of the government through GSA’s wireless solution, right sizing of services and pooling of mobile device minutes
11. Baseline agency usage and eliminate unnecessary inventory and service
12. Compliance-focused procurement support and full understanding of the FAR and Federal requirements, including Buy American, Trade Agreements, Advance Notice and Consent, Section 508, etc.
13. Established processes for expediting orders and deliveries, and for escalation of order issues
14. Procurement of mobile devices at least one generation behind the most current release unless the latest model can be procured at no additional cost
15. Provide Device Activation services
16. Device activation of new or existing lines
17. Activation of upgraded or loaner devices
18. Provide Device Return services, including the return and destruction of devices that are either damaged or at the end of their useful life
19. Provide Technical Support services to include:
20. Service suspension
21. SIM swaps (moving phone number to a SIM card)
22. Verify type of service (international vs. domestic)
23. Verify upgrade eligibility with provider
24. Provide Executive Support
25. Perform Break Fix Support
26. Provide Expense Management services to include:
27. Management of existing lines of service through: right-sizing of minutes/data allocation amongst users, pooling of minutes/data, billing review and/or other innovative approaches
28. Reports that provide visibility into the number of orders, number of lines, number of lines activated, number of lines deactivated and usage
29. Report availability by user, and other DoS organization units (e.g. Division, Office, Bureau, etc.)
30. Provide Mobile Device Deployment Support, including:
31. Procure demo units for testing
32. Package and shipping of mobile devices
33. Tracking of mobile devices and components received and transferred
34. Order processing and inventory reports
35. Staging and kitting of mobile devices
36. Procurement of mobile devices and components
37. Provide Reporting and Business Intelligence services, including:
38. Ongoing usage management and analysis
39. Asset management and tracking
40. Report all mobile service usage and pricing data to Integrated Data Collection
41. Expense validation
42. Service plan optimization
43. No Added Charge Domestic Mobile Capabilities
    * + 1. Additional Mobile Services

The Contractor shall manage the services below at no additional charge to the Government.

1. International Roaming capabilities, and ability to activate per Government request
2. International Long Distance Toll Restrictions ─ The Government shall be able to disable international long distance calling that will result in additional toll charges
3. Device Accessories: AC Charger, Headset, Holster, Car Charger, and Case
4. Unlimited Short Messaging Services (SMS)
5. Blocking of all pay per call/minute services (such as 900, 976)
6. Wireless hands-free capability with FIPS 140-2 and NIST 800-121 compliant encryption
7. Remote suspend/resume, kill, and wipe functionality
8. Call waiting and Caller ID
9. Three-way conference calling and call forwarding
10. 911 emergency services
11. Unlimited nights and weekends
12. Service packages that allow for the sharing of minutes each month by all phones.
13. Access to a device Risk Management module for better management of mobile devices
14. Ability to seamlessly transition from digital to analog systems when roaming.
15. Ability to change or cancel the service plan at any time by contacting the Contractor
16. Ability to receive messages when out of service or out of range. When back in range of service, the phone must reflect any waiting voicemail messages via message tone and visual indication
17. Ability to receive paging over an Internet-based system
18. Global System for Mobile Communications (GSM) and/or Code Division Multiple Access (CDMA) phone service. Additionally, service for all phones, must have data communications capability
19. Detailed billing per phone
20. Transfers of existing Government phone numbers to new devices
21. Newly introduced equipment into the program, the Contractor shall allow the Government to test all devices for a period for up to sixty (90) days before purchasing.
22. There shall be no roaming or long distance charges for domestic calls
23. The pooled-minute plan shall be automatically readjusted to the billing plan that is most cost-effective for the Government
    * + 1. International Mobile Services

The Contractor shall manage voice, text and data services (“Mobile Services”) to employees internationally on a 24x7x365 schedule to include procurement support for services and service enabling devices. The list of international locations serviced can be found in the appendix. In addition to voice, text, and data services, the contractor shall manage additional international mobile services

The contractor shall:

1. Provide fulfilment and return services for mobile devices
2. Invoice Reporting services, including:
   1. Invoice reporting available on the contractor website
   2. Maintain detailed logs and transactional records for auditing purposes
3. Service Ordering services, including:
4. Ordering and disconnection of voice, text and data services
5. Web-based self-service tool for ordering devices and service
6. Device Ordering services, including:
7. Support the ordering of new and replacement devices
8. Have established agreements and provide considerable savings through volume discounts with industry-leading mobile device manufacturers and cellular service providers
9. Leverage the buying power of the government through GSAs wireless solution, right sizing of services and pooling of mobile device minutes
10. Baseline agency usage and eliminate unnecessary inventory and service
11. Compliance-focused procurement support and full understanding of the FAR and Federal requirements, including Buy American, Trade Agreements, Advance Notice and Consent, Section 508, etc.
12. Procurement of mobile devices at least one generation behind the most current release unless the latest model can be procured at no additional cost
13. Established processes for expediting orders and deliveries, and for escalation of order issues
14. Device Activation services, including:
15. Device activation of new or existing lines
16. Activation of upgraded or loaner devices
17. Device Return services, including:
18. Return and destruction of devices that are either damaged or at the end of their useful life
19. Technical Support services, including:
20. Service suspension
21. SIM swaps (moving phone number to a SIM card)
22. Verify type of service (international vs. domestic)
23. Verify upgrade eligibility with provider
24. Provide Executive Support
25. Perform Break Fix Support
26. Expense Management services, including:
27. Management of existing lines of service through: right-sizing of minutes/data allocation amongst users, pooling of minutes/data, billing review and/or other innovative approaches
28. Reports that provide visibility into the number of orders, number of lines, number of lines activated, number of lines deactivated and usage
29. Report availability by user, and other DoS organization units (e.g. Division, Office, Bureau, etc.)
30. Mobile Device Deployment Support services, including:
31. Procurement support for demo units for testing
32. Package and shipping of mobile devices
33. Tracking of mobile devices and components received and transferred
34. Order processing and inventory reports
35. Staging and kitting of mobile devices
36. Procurement support for mobile devices and device components
    * + 1. Mobile Engineering

The contractor shall provide professional mobile support services domestically and internationally that cover the mobile device management lifecycle. These services must be available 24x7. As technologies advance the contractor shall provide the Government innovative approaches and solutions to address the evolving requirements.

The contractor shall provide Operations and Maintenance support for the following:

1. Mobile Device Management (MDM) currently VMware Workspace ONE SaaS w/ ACCESS
2. GO Manager – Business automation, device tracking and accounting system (Built on Servicenow platform)
3. MobiChord – Telecommunications Expense Management
4. Mobile Lifecycle Management (MLM) services
   * 1. Refresh and IT Move Support

Refresh and IT Move support includes the upgrade and modernization (refresh) of endpoints and peripherals IAW IRM and bureau agreed timelines/schedules in the NCR as well as Domestic locations.

The Contractor shall:

1. Image endpoints before deployment with the most current SOE-D image and patches.
2. Use Government Furnished tools for ticket logging & handling.
3. Update tickets IAW the Enterprise Incident Management Guide and DOS Incident Management Process guide for trend analysis and ticket resolution.
4. Follow asset and configuration procedures and policies for equipment installation, replacement and disposition.
5. Follow change procedures and policies for equipment, installation, replacement and disposition.
6. Provide disconnect/reconnect support (IT Moves) during core and after-hours and coordinate those activities within approved resources targets.
7. Manage IT Moves as projects based on complexity with a schedule.
8. Manage both refresh and IT moves schedule.
9. When not engaged in refresh or IT Moves these resources will assist other task areas such. This will be coordinated with and approved by the COR and the contractor must ensure proper cost allocation is performed.
10. Report refresh and IT Moves activities and update and maintain resourcing levels in the IMS.
    * 1. GFE Management

IRM will provide the contractor with GFE that enables service delivery. The contractor shall be responsible for the accountability, O&M, and lifecycle management of the GFE.

* + - 1. GFE Accountability and Management

The contractor shall adhere to asset and configuration processes as outlined in 14 FAM and 14 FAH. The contractor must comply with all FAR, Department of State Acquisition Regulation (DOSAR), IRM regulations, guidelines, and procedures governing GFE

The contractor shall:

1. Perform duties as Equipment Custodian. The contractor shall perform annual and periodic partial inventory audits that are validated against Government SLAs.
2. Perform Inventory IAW FAM & FAH in the NCR as well as Domestic locations.
3. Perform physical asset audits to validate inventory IAW FAM & FAH policy, guidelines, and procedures as well as IRM supplemental procedures in the NCR as well as Domestic locations.
4. During the performance of this task order at an unknown time, new inventory reconciliation processes and tools may reduce the requirements for physical inventory. Once known, a change order will be requested to reduce or remove the requirements of this task.
5. Prepare an Asset Audit Reports to include:
6. Hardware data elements.
7. Software data elements.
8. Perform other audits to validate configuration items as well as asset reconciliation.
9. Maintain GFE information in the CMDB and DOS inventory repository of record and reconcile between the databases.
10. Report GFE management activities in the MPSR.
    * + 1. Sparing and Asset Staging

The contractor shall:

1. Provide sparing and staging across the NCR and Domestic field offices in an efficient and cost-effective manner that minimizes mean time between failures/outages for DOS managed assets to include transportation of assets using Government provided vehicles and/or coordination of GSA approved transportation vendors.
2. Establish and maintain minimum stocking levels at designated sparing locations to support high operational uptime.
   * + 1. Equipment Disposition

The contractor shall:

1. Properly dispose of all obsolete, excess, or surplus equipment, hardware, and software at contractor or Government facilities IAW applicable laws and regulations.
2. Adhere to FAM, FAH and IRM guidance for disposition of obsolete (or no longer needed) GFE.
3. Update repositories of record.
4. Coordinate pick-up and transportation of equipment for disposition using Government provided vehicles and/or coordination of GSA approved transportation vendors.
5. Report activities in MPSR. 
   * + 1. GFE Maintenance and Agreements

The contractor shall:

1. Provide maintenance, parts replacement and warranty support.
2. Provide hardware warranty support for on-site repairs and off-site coordination.
3. Maintain a warranted item log and provide trend analysis for issues with GFE.
4. Maintain accurate maintenance agreements information in the CMDB.
5. Report maintenance and warranty issues which could affect DOS operations.
   * 1. User Account Support & Directory Service Support

The contractor shall:

1. Manage all objects within the consolidated Active Directory (AD) structures.
2. Maintain IRM AD along with consolidated AD structures, as required.
3. Manage access control to the Consolidated Administrators group.
4. Maintain and update: OU plan and design documentation and the Consolidated Group Policy.
5. Provide support for Local and privilege-level user account.
6. Creation, maintenance and deletion of SBU accounts.
7. Creation, maintenance and deletion of Classified accounts.
8. In-bound and out-bound transfers of SBU accounts.
9. In-bound and out-bound transfers of Classified accounts.
10. Manage security patches and antivirus signatures on IRM servers.
11. Assume operational responsibility for additional AD structures as necessary.
12. Perform audits to ensure quality as well as FISMA compliance.
13. Report AD activities.
14. Adhere to Security Management processes as outlined in the FAM and FAH.
    1. Task Area 3: IT Service Management

IT service management includes all processes required to manage the end-to-end delivery of IT services to the Department’s customers. IRM has adopted ITIL as its service management model and expects to further develop and mature the ITIL practices and processes, with assistance from the contractor. The Contractor shall apply and adapt the best practices for ITSM as the basis for managing and operating Customer Support and Mobile Services, systems, and processes. ITSM provides a structured approach for managing the services and processes in this task order.

* + 1. Service Management Practices

The IT Service Management Plan describes how the contractor will align their service support and delivery to the ITIL model and the DOS framework”.

The Contractor shall:

1. Create, update, enhance, and maintain an IT Service Management Plan describing the Service Management System, how ITSM will be managed, supporting policies, and the overall service delivery for Customer Support and Mobile Services. This federated plan will build from current DOS plans that outline the processes, roles, and responsibilities, associated technologies, and SLA/SLOs/KPIs tied to each of practices/processes/services and their integration into higher IRM Enterprise plans and processes.
   * 1. Availability Management

Availability Management ensures Customer Support and Mobile Services deliver agreed levels of availability to meet the needs of customers and users.

The contractor shall:

1. Ensure availability for Customer Support and Mobile Services while accounting for service continuity.
2. Ensure availability is measured in terms of customer experience and not merely IT centric measurements such as mean time to restore service (MTRS).
3. Document current services availability and if necessary, create plan to adjust the availability to meet business/customer requirements.
4. Design services to meet availability requirements as defined in corresponding SLA.
5. Recommend improvements or upgrades to infrastructure, systems, third-party supplier agreements or other resources to meet business requirements and DOS SLAs.
6. Report service and underpinning resources availability at a minimum at the MPSR.
   * 1. Business Analysis

Business analysis aims to solve or refine specific business needs or issues with the goal of facilitating better value creation for stakeholders.

The contractor shall:

1. Perform data analysis and data modeling for Customer Support and Mobile Services.
2. Recommend enhancements to include service delivery and process improvements based on data analysis which improve warranty and utility.
   * 1. Capacity and Performance Management

Capacity and Performance management includes satisfying current and future demand in a cost-effective way to ensure services achieve agreed and expected performance.

The contractor shall:

1. Ensure all Customer Support and Mobile Services (new and existing) meet capacity and performance requirements outlined with the corresponding SLA and underpinning resources that can support the service.
2. Coordinate demand management and its effects on resource capacity.
3. Monitor component performance and or other resources to include human capital and provide analysis of proposed changes to current infrastructure and resources.
4. Ensure that performance measurements and reporting is at the service level, from the customer perspective not just component performance.
5. Report service and underpinning resources capacity at a minimum at the MPSR.
   * 1. Change Enablement

Change enablement maximizes the number of successful IT changes by ensuring risks are properly assessed, changes to proceed are authorized, and change schedules are managed.

The contractor shall:

1. Implement and maintain change management processes for Customer Support and Mobile Services that adhere to Enterprise Change Management processes/policies/guidelines.
2. Manage all changes to Customer Support and Mobile Services and infrastructure ensuring the lowest level of risk through risk assessments.
3. Prioritize, review and assess all Change Requests/Request for Change.
4. Evaluate all changes for quality and completeness.
5. Participate in Government-run review boards such as Change Advisory Board (CAB) to authorize all changes as required.
6. Ensure all changes are recorded in the Configuration Management System (CMS).
7. Ensure all changes are approved before deployment.
8. Ensure all changes are scheduled and the schedule is current and available to stakeholders.
9. Ensure that service validation and testing has been performed for any proposed changes and coordination has been done for release and deployment as necessary.
10. Evaluate incidents to ensure Change Requests/Request for Change are submitted as required.
11. Provide reports on change activity.
12. Complete Post-Implementation Reviews (PIR) for changes that require PIRs.
13. Ensure changes are properly reflected in Continuity of Operations Plan (COOP) and Disaster Recovery (DR) as necessary.
    * 1. Incident Management

Incident management minimizes the negative impact of incidents by restoring normal service operations as quickly as possible. The requirements below address how the contractor will manage incidents related to Customer Support and Mobile Services. The contractor will also manage and coordinate the handling of IT incidents Department-wide via the processes detailed in section 2.2.1 Customer Contact Handling / IT Service Desk Support.

* + - 1. Incident Management Practice

The contractor shall:

1. Implement and maintain processes for incident management that adhere to Enterprise Incident Management processes/policies/guidelines.
2. Log, categorize, prioritize, allocate, track, and escalate incidents. Provide the status and summary of incidents in the MPSR.
3. Respond to incidents and notify the Government as necessary such as in the case of escalation.
4. Report major incidents, provide notification and updates until resolution.
5. Proactively monitor incidents for trends and triage with affected service areas.
6. Use Government provided tool as the incident repository.
7. Ensure that the notification about unscheduled maintenance is posted IAW SLAs.
8. Communicate scheduled maintenance notification IAW SLAs.
9. Communicate information about known issues/outages and their anticipated resolution times as described in the SLAs.
10. Collaborate with other DOS service providers as well as third-party and XaaS service providers to facilitate rapid incident resolution.
11. During the performance of this task order at an unknown time, new ITSM tool functionality may reduce the requirement for this task. Once known, a change order will be requested to reduce or remove this task.
    * + 1. Incident Analysis

The incident resolution process involves both immediate assistance to the end users and analysis of the encountered issues. To increase efficiency of employed systems and to minimize disruption to the ongoing operations, the Government expects incident analysis to decrease response times, maintain user satisfaction, quickly restore normal operations, and reduce the occurrence of incidents in the future.

The contractor shall:

1. Provide initial diagnosis, when possible leveraging Knowledge Management.
2. Provide recommendations that are not limited to technical solutions only, but shall also incorporate suggestions for improving internal processes, as appropriate.
3. Open problem tickets for incidents depending on the nature and/or frequency of the incident(s).
4. Present the summary results of incident management, along with recommendations for improvement, on a regular basis as part of the standard MPSR.
   * 1. IT Asset Management

IT Asset Management is utilized to plan and manage the full lifecycle of all IT assets, to help the organization maximize value; control costs; manage risks; support decision-making about purchase; re-use, and retirement of assets; and meet regulatory and contractual requirements.

The contractor shall:

1. Implement and maintain processes for the management of Customer Support and Mobile Services assets/configuration items that adhere to Enterprise Asset and Configuration Management processes/policies/guidelines found in 5 FAM and 14 FAM as well as 12 FAH and 14 FAH.
2. Manage all consolidated GFE from delivery to disposal.
3. Provide license management for DOS applications and software.
4. Audit assets, license usage and consumption to include PaaS, IaaS and SaaS tools and service components.
5. Ensure all IT assets including cloud assets are identified and current in the CMS as well as DOS trackable asset registers.
   * 1. Monitoring and Event Management

Monitoring and event management includes systematically observing services and service components and recording and reporting selected changes of state identified as events, through identifying and prioritizing infrastructure, services, business processes, and information security events, and establishing the appropriate response to those events, including responding to conditions that could lead to potential faults or incidents.

The contractor shall:

1. Implement and maintain processes for Customer Support and Mobile Services-related event management that adhere to IRM Enterprise Event Management processes/policies/guidelines. Customer Support and Mobile Services is not the process owner but is a stakeholder in the execution of event management across the DOS.
2. Ensure DOS components and services have event notification capabilities, to include automated notification based on Government approved thresholds with tie-ins to the ITSM tool.
3. Log and communicate event notifications IAW Government approved policies and procedures to customers and stakeholders.
4. Provide data to support severity notification (SEV) IAW IRM outage requirements.
5. Report any events in the MPSR to include:
6. Total number of events for the reporting period.
7. Summary and analysis of the event triggers that resulted in incidents for the current reporting period.
8. Problems nominated because of events.
9. Monitor all DOS services including individual components/configuration items that aggregate to provide DOS services.
10. Monitor DOS assets for security policy violations.
11. During the performance of this task order at an unknown time, new ITSM tool functionality may reduce the requirement for this task. Once known, a change order will be requested to reduce or remove this task.
    * 1. Problem Management

Problem management involves identifying actual and potential causes of incidents, and managing workarounds and known errors to reduce the likelihood and impact of incidents. The requirements below address how the contractor will manage problems related to Customer Support and Mobile Services. The contractor will also manage and coordinate the handling of IT problems Department-wide via the processes detailed in section 2.2.1 Customer Contact Handling / IT Service Desk Support.

* + - 1. Problem Management Practice

The contractor shall:

1. Liaise with the Government points of contact (POCs) to ensure subject matter experts (SME) are providing problem management support.
2. Facilitate joint service provider resolution sessions to resolve problems and provide recommendations to the Government.
3. Implement, maintain, and enhance Problem Management processes and activities that adhere to IRM Enterprise Problem Management process/polices/guidelines.
4. Identify, monitor, diagnose, mitigate, record and report problems.
5. Perform pro-active trend analysis on event and incident data.
6. Perform reactive problem management on availability, capacity and demand, event, incident, and Government-provided data.
7. Establish and track problem records in the Problem Management tracking tool to relate incident or event data and document problem artifacts.
8. For errors that can be resolved, permanent resolution is the goal. All workarounds shall be re-evaluated for possible permanent resolution.
   * + 1. Problem Analysis

The contractor shall:

1. Conduct problem analysis on all Customer Support and Mobile Services problem tickets.
2. Perform root cause analysis (RCA) using structured approaches, such as Kepner-Tregoe, using appropriate analysis techniques to identify the underlying cause of the problem, its overall impact, and solutions for eliminating this cause in the future.
3. Document RCA methodology and ensure that every problem ticket is updated with information about the root cause of the problem.
4. Develop workarounds and update the Known Error Database (KEDB) with known errors, workarounds, and solutions.
5. Determine resolution and create Request for Change (RFC) to resolve problems.
6. Test and vet proposed solution through the change management process before releasing into production.
7. Support problem analyses of known errors detected during development and ensure those that are released into production are logged in the KEDB.
8. Report problem review reports/problem closeout.
   * 1. Release Management

Release management involves making new and changed services and features available for use.

The contractor shall:

1. Be responsible for release planning and supporting processes for all Customer Support and Mobile Services-related changes to the production environment.
2. Provide service or change functionality for deployment at a later time.
3. The contractor shall institute an Agile/DevOps service/product release model.
4. The contractor shall determine which deployment model is appropriate e.g., waterfall or Agile/DevOps based on the criteria.
5. Schedule all releases and coordinate the releases with the appropriate stakeholders.
6. Transition design packages/changes/projects to Service Release Packages (SRPs) for new, changed or retired services upon approval from the CAB. The SRP shall at a minimum include:
7. Release technical description.
8. Release site(s) location(s).
9. Release Plan of Action and Milestones (POA&M).
10. Release build and test operational and verification plan.
11. Plan for user and organization communications (as required).
12. Plan to update all affected documentation including site drawing packages; integrated architecture, engineering, and operations supporting documentation; asset data; and Configuration Items (CI) in the CMS.
13. Identify risks and mitigation strategies.
14. The contractor shall conduct post-implementation reviews and coordinate the resolution of the ticket with change management.
    * 1. Service Catalog Management

Is the Business Owner for Service Catalog Management provides a single source of consistent information on all services and service offerings, and ensures that it is available to the relevant audience. The contractor under this task order is not responsible for the strategy and management of IRM’s Service Catalog; however, the contractor will participate in meetings, discussions and development of services and service catalogs representing DOS service delivery and the customer perspective.

The contractor shall:

1. Improve, maintain and update DOS’s Service Catalog hosted in DOS SharePoint and ITSM tool and service portal with all relevant data.
2. Support the development of a catalog with different views: User, Customer and Business to Business (B2B).
3. Support updates to the ITSM service portal including the request catalogue and Tier 0 capabilities and other knowledge such as FAQs.
4. Identify new opportunities for self-help and transition those to the service portal and/or FAQs.
   * 1. Service Configuration Management

Service Configuration Management ensures that accurate and reliable information about the configuration of services, and the configuration items (CIs) that support them, is available when and where it is needed. This includes information on how CIs are configured and the relationships between them.

The contractor shall:

1. Manage, maintain, update, and enhance the CMS for all consolidated Bureau CIs and their relationships to other CIs and artifacts.
2. Ensure CIs relationships are accurate in the ITSM tool and Configuration Management Database (CMDB) and update CI data.
3. Process artifacts, such as incident, problem, and change records.
4. Develop and perform Configuration Audits in coordination with operations to verify the information in the CMS is the same as in production.
5. Ensure that the COOP/DR is updated to reflect changes in asset and configuration
6. Collect CI data and provide configuration status and CI status reports.
7. Ensure configuration settings for DOS managed assets, systems, environments and services adhere to FIPS 200 and NIST SP 800-53.
   * 1. Service Continuity Management

Service Continuity Management ensures the availability and performance of a service is maintained at a sufficient level in the event of a disaster. The practice provides a framework for building organizational resilience, with the capability of producing an effective response that safeguards the interests of key stakeholders and the organization’s reputation, brand, and value-creating activities.

The contractor shall:

1. Design, maintain, update, and enhance DOS’s business continuity for all Customer Support and Mobile Services detailed in Continuity of Operations Plan (COOP) and demonstrated Disaster Recovery (DR) capability to maintain the same level of operational support and ensure that the alternative capability meets SLAs and COOP guidelines.
2. Coordinate the design and enhancement of services to ensure service, practice and process continuity.
3. Ensure the alternate systems are:
4. Maintained with the same software release levels and patches as the primary systems adhering to Release Management processes.
5. Configured with the same configuration information as the primary systems adhering to Configuration Management processes.
6. Capable of operating on their own in case of partial or full failure of the primary systems.
7. Develop, maintain, test, and execute a COOP during emergency or training situations
8. Execute COOP exercises and real-world scenarios IAW COOP to include the following elements:
9. Maintain operational support by using tools and systems available from alternative sites and, if applicable, contractor’s facilities and/or resources.
10. Provide support activities using the alternate facilities for the duration of the outage/exercise.
11. Transition operations back to the primary support location.
12. Update primary operational and support tools and systems with data collected and updated during the outage.
13. Initiate operations from the primary site.
14. Re-sync primary and alternate systems.
15. Stand down the alternate operations.
16. Develop, test, and maintain a Disaster Recovery Plan IAW IRM COOP and NIST SP 800-34.
17. Maintain and operate alternative sites’ tools service the same as the primary site as a result of new or changed services, support directives, or security mandates adhering to Release and Configuration management practices.
18. Develop, maintain, test, and implement back-up and restore SOPs and job-aides/work instructions and maintain off-site backups in coordination with Knowledge Management.
19. Ensure that service owners have planned and documented the necessary alternative site resource requirements and that these are periodically reviewed and tested
20. Provide an After-Action Report (AAR) in the event of an outage, disaster, or exercise.
    * 1. Service Design

Service Design includes designing products and services that are fit for purpose, fit for use, and that can be delivered by the organization and its ecosystem. This includes planning and organizing people, partners and suppliers, information, communication, technology, and practices for new or changed products and services, and the interaction between the organization and its customers.

The contractor shall:

1. During the POP it is expected that new Customer Support and Mobile services will be created, changed or retired that the contractor may design, implement and manage.
2. Design new and existing services for continuity.
3. Incorporate Human-centered/Customer Experience (CX) or User-centered/User experience (UX) design into new or existing services as the service/scenario warrants.
4. Service design will use Agile/DevOps models for service creation and enhancements/changes as these changes move through the service value system.
   * 1. Service Level Management

Service Level Management sets clear business-based targets for service performance, so that the delivery of a service can be properly assessed, monitored, and managed against these targets.

The contractor shall:

1. Deliver Customer Support and Mobile Services IAW SLAs established under this task order. The objective is to continuously refine SLAs corresponding SLOs/metrics during the performance on this task order. SLOs/metrics will be updated, added, or retired as approved by the Government.
2. Design new and update existing services with specific service levels and critical success factors (CSFs) defined at project conception and agreed to by IRM and project stakeholders.
3. Draft new or update existing SLAs for all services. SLAs and corresponding SLOs/metrics must be from the customer perspective that take a holistic view of service delivery not merely simplistic operational component based or percentage availability measurements.
4. Report and monitor SLAs, SLOs, metrics, and KPIs in the MPSR.
5. The contractor shall submit SLO/SLA data to appropriate IRM offices as directed by the COR.
6. Develop and maintain Operational Level Agreements (OLAs) identifying roles, responsibilities, and resources required.
7. Draft new or update measurements, metrics, and KPIs with an emphasis on availability, reliability, and performance for services in coordination with Service owners and CSI.
8. Coordinate Service Level Management (SLM) with CSI activities including proactively audit service and process owners for compliance with SLAs and SLOs.
9. Draft service guides for all DOS services and maintain this documentation.
10. Conduct at a minimum, semi-annual service review meetings to report on service levels and end-to-end performance. Changes to services may warrant additional reviews.
11. The contractor shall be responsible for gathering, processing, and presenting the SLA data at the regularly scheduled review session.
    * 1. Service Request Management

Service Request Management supports the agreed quality of a service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner. The requirements below address how the contractor will manage service requests related to Customer Support and Mobile Services. The contractor will also manage and coordinate the handling of IT service requests Department-wide via the processes detailed in section 2.2.1 Customer Contact Handling / IT Service Desk Support.

The contractor shall:

1. Implement, maintain, and enhance Customer Support and Mobile Service Request Management processes and activities that adhere to IRM Enterprise Request Management process/polices/guidelines.
2. Manage the life cycle of all service requests from users.
3. Improve service request processes.
4. Provide innovative solutions to manage service requests to include self-service options, automation, etc.
5. Report on the request management processes and activities and SLOs.
   * 1. Service Validation and Testing

Service Validation and Testing ensures that new or changed products and services meet defined requirements. The definition of service value is based on input from customers, business objectives, and regulatory requirements, and is documented as part of the value chain activity of design and transition. These inputs are used to establish measurable quality and performance indicators that support the definition of assurance criteria and testing requirements. The contractor is responsible only for validation and testing of services and systems under the purview of this PWS.

The contractor shall:

1. Establish acceptance criteria for Customer Support and Mobile Services using both utility and warranty customer requirements.
2. Establish and maintain a development, integration, test, and validation model that emulates the production environment either using IRM’s enterprise environment or create an environment that supports DOS’s requirement.
3. Use the Enterprise environments or DOS environments to test enhancements/new configurations of the current systems and/or test replacement equipment and systems.
4. Provide a separate “test” resources with management controls to ensure adequate integrity of the testing processes.
5. Place emphasis on pre-deployment testing of new tools, updates, and patches, including roll-back procedures and simulation.
6. Use an empirical approach in testing.
7. Validate Consolidated Bureau application SOE-D compatibility.
8. Report test results to change management.
9. Perform Utility tests: Unit, system, integration, and/or regression.
10. Perform Warranty tests: Performance & capacity, security, compliance, operational, and/or user acceptance.
    * 1. Deployment Management

Deployment Management involves moving new or changed hardware, software, documentation, processes, or any other component to live environments. It may also be involved in deploying components to other environments for testing or staging.

* + - 1. General Deployment

The contractor shall:

1. Make releases available to the user environment.
2. Determine the appropriate deployment approach based on the service, asset or component type as well as the criticality of the deployment for all Customer Support and Mobile Services tasks.
3. Maintain the definitive media library.
4. Create communications plans for all deployments appropriate to the deployment type including KPIs. The Government will approve all communications plans.
5. Liaise with external stakeholders and suppliers to successfully implement deployments such as software vendors, hardware vendors, SaaS, IaaS and PaaS.
6. Provide early life support for deployed changes.
   * + 1. Standard Operating Environment

The contractor shall:

1. Coordinate Standard Operating Environment for Desktops (SOE-D) updates between the Enterprise and Bureau specific applications including supporting Bureau testing and pilots by providing administrative privileges and limited guidance.
2. Manage DOS software library for various vendor platforms to support the SOE-D.
3. Manage SOE-D Consolidated Bureau application deployments.
   * + 1. DOS Server Management

The contractor shall:

1. Provide DOS server security management for both SBU and Classified servers and systems.
2. Maintain current anti-virus definition files on DOS managed equipment.
   * + 1. DOS IT Asset Security Management Deployment

The contractor shall:

1. Maintain current anti-virus definition files on DOS managed equipment.
2. Provide SBU and Classified Secret endpoint security management.
3. Monitor vulnerabilities and apply security patches IAW Cyber Operations (CO), DS guidelines.
   * + 1. Classified Operating Environment

The contractor shall:

1. Deploy updates to the Classified Environment image.
   1. Task Area 4: Project and Surge Support

The contractor shall provide project support for introducing new services to operations, which will then become O&M support after an appropriate transition timeframe.

Definite requirements will be addressed in a Request for Proposal/Request for Quote RFP/RFQ as a modification to the task order.

Projects/surges must address and incorporate ITIL 4 framework, project/surge approach and execution.

* 1. Task Area 5 Special Projects and Subject Matter Expert Support

The Contractor shall provide subject matter expertise capable of advising IRM, IRM Offices, and Division/Branch Chiefs on services, techniques, and technology capable of supporting and enhancing the mission.

Such services may include in-depth technology analyses, development of white papers, reports, and briefings, establishment of working groups, and development of new business processes and procedures leading to improved efficiencies.

* 1. Task Area 6: Cross-Functional Requirements

The following table summarizes the Cross-Functional categories that all contractors are required to support across each task order.

1. Cross Functional Requirements

| Requirements Category | Description |
| --- | --- |
| Compliance | IT Compliance resources setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. Includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery. |
| Security | IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cybersecurity & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security |
| Disaster Recovery | IT Disaster Recovery resources setting DR Policy, establishing process and means, dedicated failover facilities, performing DR testing: NOTE: DR designated equipment is included directly in its own sub-tower (e.g., extra servers for DR are included in Compute tower, etc.). |
| Client Management | Resources or “account managers” aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects. |
| IT Service Management | Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier I help desk). |
| Product and Project Management | Resources involved with managing and supporting IT related projects and/or continuous product development (e.g., Agile) across business and IT-driven initiatives. |
| Innovation, Ideation, and Modernization | The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services.  Includes enterprise architecture solutions that enhance and modernize DOS services. |

* + 1. IT Compliance

IT Compliance resources include setting policy, establishing controls and measuring compliance to relevant legal and compliance requirements. This includes but is not limited to: Governance, Risk & Compliance, Business Continuity & Disaster Recovery.

The Contractor shall:

1. Comply with all relevant certification and accreditation requirements and documentation specified by DOS and the U.S. Government.
2. Adhere to policies and procedures defined in the Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAHs) to include, but not limited to proactively reporting non-compliance issues and risks.
3. Participate in compliance, risk and regulatory governing bodies, processes and activities as required.
4. Measure (or provide inputs needed to support measurement of) compliance to relevant legal and compliance requirements.
5. Monitor all work performed by assigned Contractor personnel to ensure the ongoing and continuous incorporation of and adherence to all appropriate Compliance requirements.
6. Report on compliance in coordination with other DOS stakeholders and/or Contractors.
7. Support remediation of compliance discrepancies as directed.
8. Support the definition and establishment of controls to monitor compliance.
   * + 1. 508 Compliance

The Contractor shall ensure the system is compliant with Section 508 throughout the implementation and integration of the work to be performed. The Contractor shall ensure the system is compliant with all appropriate 508 requirements and lead the testing and validation for every major and minor release. In the event that a user with disabilities identifies a defect with 508 compliance the Contractor must accommodate appropriately. Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C.794d) requires that when Federal agencies develop, procure, maintain, or use electronic information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who do not have disabilities, unless an undue burden would be imposed on the agency.

Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency.

Applicable standards are 1194.211194-26.

Implementation Instructions

* <http://www.section508.gov/content/learn/laws-and-policies>
* <http://www.access-board.gov/508.htm>
* <http://www.w3.org/WAI/Resources>
  + 1. Security

IT Security resources setting policy, establishing process and means, measuring compliance and responding to security breaches. Includes Identity & Access Management, Security Awareness, Cybersecurity & Incident Response, Threat & Vulnerability Management, and Data Privacy & Security.

If the Contractor becomes aware of any unauthorized access to the Governments information or a security breach that compromises or reasonably could compromise Government information (an “incident”), the Contractor shall take immediate action to contain the incident, in accordance with applicable law and Department of State policies and procedures, and notify the Government, to include CIRT@state.gov, and the COR, as soon as reasonably possible. The Contractor shall provide the Government with information regarding any incident as may be reasonably requested by the Government and that is in the Contractor’s possession, custody, or control at the time a request is received. Upon request of the Government, the Contractor shall cooperate with the Government to investigate the nature and scope of any incident and to take appropriate actions to investigate and otherwise respond to the incident or associated risks. (As used in this Section, “compromise” means that the information has been exposed to any unauthorized access, inadvertent disclosure, known misuse, or known loss, alteration or destruction of Confidential Information other than as required to provide the services)

* + 1. Security Management

Security management follows the most current version of NIST publications including FIPS 199, 200 and SP 800 18,37, 53, 181 NISPOM DoD 5220.22-M, DOS policies and procedures including 5 FAH-11, 12 FAM and 12 FAH and statutory law including Federal Information Security Management Act (FISMA).

1. Personnel providing security management tasks/roles must obtain one of the baseline certifications from DoD 8570.01-M based on their job function/tasks assigned. The contractor must provide a matrix for these personnel in the staffing plan with justifications on why they have selected those criteria e.g., IAM/IAT levels, NICE roles to meet the security management requirements in the PWS. DOS has specific, mandatory cybersecurity/information assurance training requirements in addition to those outlined in DoDD 8140.
2. Develop and maintain Security Management dashboard to track all activities in this task.
3. Develop and use a case management system to task, track and report security management requests such as Assessment and Accreditation (A&A) status, Freedom of Information Act (FOIA), Office of Inspector General (OIG), Computer Incident Response Team (CIRT), legal, etc. This case management system will be GFE.
4. Continuous monitoring and tracking of CCS and consolidated bureau systems, environments, services, assets and off-premise/cloud platforms for compliance with information security policies, FIPS procedures and guidelines.
5. Audit CCS and consolidated bureaus systems, environments, services, assets and off-premise/cloud platforms for compliance with information security policies, procedures and guidelines.
6. Manage and perform A&A for CCS applications, systems and environments including Security Authorization packages.
7. Create and submit appropriate security-related reports, such as intrusion, security breaches and incidents and FISMA requirements.
8. Report CCS and Consolidation Bureaus’ security compliance to higher level authorities and/or reporting structures.
9. Support and validate access requests for DOS SBU and Classified networks, Managed services and DOS cloud platforms.
10. Provide oversight to ensure that closed areas of CCS comply with NISPOM, 12-FAM-500, 12-FAM-600 and 12-FAH-10.
    * 1. Device Security

Any Government owned, approved, and issued mobile devices must use hardware and software approved by the Government’s internal change control board, which includes all relevant security stakeholders. The Government and other agency officials must implement technical and non-technical safeguards in accordance with guidance issued by the National Institute of Standards and Technology (NIST). These safeguards are approved and monitored by the Department’s Diplomatic Security bureau.

* + 1. Ownership of User Data

The Government will own all user data, including the name of the individual using the service, all contact information, usage information and inventory data. The Government will also own all content sent to the Government including emails, text messages, data, and voice mails.

* + - 1. Information Technology Security Plan

In accordance with Dept of State Acquisition Regulation (DOSAR) clause 652.239-71(b), the contractor shall develop, provide, implement and maintain an IT Security Plan.

* + - 1. Cybersecurity

Cybersecurity is mandatory for all task orders placed under the Evolve contract. The objective of the cybersecurity requirement is to ensure that all task orders placed under the Evolve IDIQ not only comply with DOS standards but go above and beyond those requirements to consider how to make DOS systems more resilient and secure in the face of continuously changing threats. The following are the current cybersecurity standards, frameworks and policies that will apply at the task order level as applicable. These lists are not all inclusive and are subject to change:

1. Federal Information Processing Standards Publications

| Federal Information Processing Standards Publications (FIPS Pub) | Reference |
| --- | --- |
| Security Requirements for Cryptographic Modules | FIPS Pub 140-3 |
| Standards for Security Categorization of Federal Information and Information Systems, February 2004 | FIPS Pub 199 |
| Minimum Security Requirements for Federal Information and Information Systems, March 2016 | FIPS Pub 200 |
| Personal Identity Verification of Federal Employees and Contractors,” January 24, 2022 | FIPS Pub 201-3 |

1. National Institute of Standards and Technology Publications

| National Institute of Standards and Technology (NIST) | Reference |
| --- | --- |
| Guide for Applying the Risk Management Framework to Federal Information Systems:  A Security Life Cycle Approach, June 10, 2014 | NIST SP 800-37 |
| Security and Privacy Controls for Federal Information Systems and Organizations, January 22, 2015 | NIST SP 800-53 Rev. 4 |
| A Recommendation for the Use of Personal Identity Verification (PIV) Credentials in Physical Access Control Systems, November 20, 2008 | NIST SP 800-116 |
| Digital Identity Guidelines, June 2017 | NIST SP 800-63-3, 800-63A, 800-63B, 800-63C |
| Guidelines for Derived PIV Credentials, December 2014 | NIST SP 800-157 |
| Guidelines on Hardware-Rooted Security in Mobile Devices (Draft), October 2012 | NIST SP 800-164 |
| Draft National Institute of Standards and Technology Interagency Report - Mobile, PIV, and Authentication, March 2014 | NISTIR 7981 |

1. Office of Management and Budget Publications

| Office of Management and Budget (OMB) | Reference |
| --- | --- |
| Managing Federal Information as a Strategic Resource,” July 28, 2016 | OMB Circular A-130 |
| Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011 | OMB Memorandum M-11-11 |
| Transition to IPv6, September 28, 2010 | OMB Memorandum |
| Acquisition of Products and Services for Implementation of HSPD-12, June 30, 2006 | OMB Memorandum M-06-18 |
| Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005 | OMB Memorandum 05-24 |
| Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007 | OMB Memorandum M-07-16 |
| Implementation of Trusted Internet Connections (TIC), November 20, 2007 | OMB Memorandum M-08-05 |
| Securing the Federal Government’s Domain Name System Infrastructure, August 22, 2008 | OMB Memorandum M-08-23 |
| Improving the Federal Government’s Investigative and Remediation Capabilities Related to Cybersecurity Incidents August 27, 2021 | OMB Memorandum M-21-31 |
| [Identity, Credentialing, and Access Management (ICAM)](https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf), May 2019 | OMB Memorandum M-19-17 |

1. Security Policies

| Security Policies | Reference |
| --- | --- |
| "Trusted Internet Connections (TIC) Reference Architecture Document, Federal Interagency Technical Reference Architectures, Department of Homeland Security, ([https://www.doi.gov/sites/doi.gov/files/uploads/tic\_ref\_arch\_v2-0\_2013.pdf](https://gcc02.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.doi.gov%2Fsites%2Fdoi.gov%2Ffiles%2Fuploads%2Ftic_ref_arch_v2-0_2013.pdf&data=04%7C01%7CWeakley-LugoKF%40state.gov%7C14aea13923b646e405db08d96bae63f1%7C66cf50745afe48d1a691a12b2121f44b%7C0%7C0%7C637659219012429211%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=YbP5%2FAfsntmTWA2EUBBBFCR5F8gVqSLDiifPXpmWiWs%3D&reserved=0)) " | Version 2.0, October 1, 2013\*Version 3 in draft |
| "Trusted Internet Connections (TIC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-05.pdf" | OMB M-08-05 |
| "Domain Name System Security (NSSEC) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2008/m08-23.pdf" | OMB M-08-23 |
| Federal Information Security Modernization Act (FISMA) of 2014 | 44 U.S.C. § ch.35 |
| Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act of 1996 | 40 U.S.C |
| Privacy Act of 1974 | 5 U.S.C. § 552a |
| Homeland Security Presidential Directive, “Policy for a Common Identification | HSPD-12 |
| Standard for Federal Employees and Contractors, August 27, 2004 |  |
| Management of Federal Information Resources, and Appendix III, | (OMB) Circular A-130 |
| Security of Federal Automated Information Systems”, as amended | OMB Circular A-130 | |
| E-Authentication Guidance for Federal Agencies | OMB Memo M-04-04 | |
| Standards for Security Categorization of Federal Information and Information Systems | FIPS PUB 199 | |
| Minimum Security Requirements for Federal Information and Information Systems | FIPS PUB 200 | |
| Security Requirements for Cryptographic Modules | FIPS PUB 140-3 | |
| Guide for Developing Security Plans for Federal Information Systems | NIST Special Publication 800-18 Rev 1 | |
| Risk Management Guide for Information Technology Security Risk Assessment Procedures for Information Technology Systems | NIST Special Publication 800-30 | |
| Contingency Planning Guide for Information Technology Systems | NIST Special Publication 800-34 | |
| Guide for the Security Certification and Accreditation of Federal Information Systems | NIST Special Publication 800-37 | |
| Security Guide for Interconnecting Information Technology Systems | NIST Special Publication 800-47 | |
| Recommended Security Controls for Federal Information Systems | NIST Special Publication 800-53 | |
| Guide for Assessing the Security Controls in Federal Information Systems | NIST Special Publication 800-53A | |
| Voice Over Internet Protocol (VoIP) Telephony | CNSSI 5000 | |
| Voice over Secure Internet Protocol (VoSIP) | CNSSI 5000 ANNEX I | |
| Softphone Security Requirements | CNSSI 5000 ANNEX J | |
| Type-Acceptance Program for Voice Over Internet Protocol (VoIP) Telephones | CNSSI 5001 | |
| Telephony Isolation Used for Unified Communications Implementations Within Physically Protected Spaces | CNSSI 5002 | |
| National Instruction for Approved Telephone Equipment | CNSSI 5006 | |
| Telephone and Security Equipment Submission and Evaluation Procedures | CNSSI 5007 | |
| Safeguarding Communications Security (COMSEC) Facilities and Materials | CNSSI 4005 | |
| Enabling Mission Delivery through Improved Identity, Credential, and Access Management | OMB Memo M19-17 | |
| Cybersecurity Strategy and implementation Plan (CSIP) | OMB Memo M16-04 | |
| Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure | E.O 13800 | |
| Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information | E.O. 13587 | |
| Instruction for National Security Systems (NSS) Public Key Infrastructure (PKI) X.509 Certificate Policy, Under CNSS Policy No. 25 | CNSSI 1300 | |

The contractor is responsible for remaining abreast of all new mandatory cybersecurity requirements at both the federal and DOS level and complying with the requirements relevant to this task order.

In addition to being able to perform in accordance to the referenced publications as required at the Task level for sensitive data and information technology (IT) resources, a contractor shall ensure that the contractor's information security policies, procedures, and practices applicable to all information systems it owns or operates which contain, transmit, or process information provided by or generated for the Government to support the operations and assets of a Federal agency (“Federal Information”), and which may be reasonably contemplated to be used during the performance of this contract, meet, at a minimum, the requirements of the security control baseline for Low-Impact information systems (in the most current version of NIST Special Publication 800-53), or conform to commercial standards requirements that provide a substantially equivalent or greater level of security.

* + 1. Disaster Recovery

Disaster Recovery services are the services and activities required to prevent and/or respond to a disaster event through the restoration of key computing functions as swiftly and smoothly as possible. A “disaster event” in this context is any event that prevents a mission-critical system from maintaining an operational state at the client production data center.

Disaster Recovery requirements under this task order are detailed under Task Area 3, section 2.3.13 - Service Continuity Management.

* + 1. Client Management

Client Management includes resources or “account managers” that are aligned with the lines of business to understand business needs, communicate IT products, services and status of IT projects.

The Contractor shall:

1. Designate a single point of contact to liaise directly with the Program Offices utilizing services delivered via this Task Order.
   * 1. IT Service Management

Resources involved with the incident, problem and change management activities as part of the IT Service management process (excludes the Tier I help desk).

IT Service Management requirements under this task order are detailed under Task Area 3. See section 2.3.

* + 1. Product and Project Management

The contractor shall provide Product and Project Management services as it relates to the work performed under this task order. Product and project management include all activities relating to the eight project performance domains identified as critical for effectively delivering project outcomes in the PMBOK® Guide (i.e., stakeholders, team, development approach and lifecycle, planning, project work, delivery, measurement, and uncertainty) and spans the full range of development approaches (agile, hybrid, predictive).

The Contractor shall perform the following task order project management activities:

1. Manage projects utilizing sound project and product management practices (i.e., Managing State Projects (MSP), Project Management Body of Knowledge (PMBOK®), and adhere to the program, project, and product lifecycle processes and standards developed by the offices.
2. Tailor the project management approach, governance, and processes to best suit the project environment. This includes selecting the approach (i.e. agile, predictive) or combination of approaches (hybrid) that is most appropriate for the unique characteristics of the project. The approach selected should consider balancing competing demands including, but not limited to, the following items:
   1. Speed to delivery
   2. Minimizing project costs
   3. Optimizing value delivered
   4. Quality of deliverables or outcomes
   5. Adhering to standards
   6. Satisfying stakeholder expectations; and
   7. Adapting to change
3. Organize and manage project team(s) into a cohesive unit to achieve mission goals and performance objectives, ensuring teams have the necessary skills to execute project activities utilizing the selected development approach for the effort.
4. IT Governance
5. Actively participate in IT Governance organizations as requested by the Government. IRM has established IT Governance organizations, policies, and procedures.
6. Develop strategies and plan recommendations that support the management of IT services.
7. Adhere to IRM IT Governance strategies, policies, and plans as they apply to the implementation and management of services and process detailed in the PWS.
8. For agile project delivery:
9. Be responsible for development teams performing the full suite of development tasks using Agile methodologies, including, but not limited to: participating in creating user stories for both business functionality, technical requirements and defining acceptance criteria; estimating the size of stories; solution design; development; and testing
10. Assist in the documentation of user stories, acceptance criteria and tasks to be completed to fulfill the definition of done for a story
11. Organize, conduct, and attend meetings
12. Collaborate with other vendors supporting the Evolve Contract and the ITS Division, to include but not limited to providing requested inputs to support internal data calls and Office of Management and Budget (OMB) reporting requirements, provide updates to project and portfolio management tools, such as ServiceNow PPM to monitor project schedules, weekly project status, etc.
13. Ensure communication is thorough, accurate, and timely to both stakeholders as well as the customer. Maintain full and open communications with the DOS COR and the Government Technical Monitors (GTM) on all matters
14. Develop, document, update, and maintain overall project artifacts in accordance with MSP-IT framework and GTM requirements
15. Develop, document, update, and maintain overall project schedules using DOS specified tools, which at a minimum includes Microsoft
16. Adhere to baselined project schedules and formally request changes to those baselines when applicable, through existing and established project review processes and/or boards
17. Identify issues and risks to project success, develop a risk management tracking log and log all identified issues / risks, along with issue/risk mitigation recommendations / plans, and facilitate
18. Provide other project management support services as required. Support and meet all established control gates, documentation, and deadlines as required by the Project Review Board (PRB), eGov PMO, IRM Executive Committee/Steering Committee.
19. Document all processes utilized in the successful execution of project management activities
20. Use the DoS designated repository for all deliverables as required
    * 1. Innovation, Ideation, and Modernization

The investment, development, and incubation of new technologies to create new or better solutions which meet unarticulated or existing market needs. Includes new technology solutions and new product incubation services.  Includes enterprise architecture solutions that enhance and modernize DOS services.

The Contractor shall:

1. Supply value engineering reports as needed.
2. Provide the most cost effective, efficient, state-of-the-art, integrated turnkey solutions while incorporating practical innovations and technologies.
3. Determine and develop best practice processes by building upon ones already in place at IRM to improve operational efficiency.
4. Identify, develop, and advance the IRM vision and strategic plan to reform IT acquisitions by bringing industry standard best practices and driving innovations.
5. Ensure IRM remains current with evolving requirements and technology advances.
6. Special Requirements/Instructions
   1. Standards (e.g., 5 FAM 600)

The Contractor shall ensure that all work is completed in accordance with U.S. government and Department of State standards, policies, procedures and guidelines as provided.

* 1. Government-Furnished Equipment / Information

The Government may furnish workspace and other appropriate furnishings, computer hardware and software, telephones and other material appropriate to the performance of tasks. Any Government furnished materials, data, or property shall remain the property of the Government and will be returned upon completion of the support services. Government furnished equipment shall be tracked through applicable procedures that will be provided by the Contracting Officer in accordance with the Federal Acquisition Regulation (FAR).

* 1. Place of Performance

Work under this task order shall be performed primarily at DoS facilities in the Washington, DC metropolitan area, including primarily State Annex (SA-34) at 7374 Boston Blvd., Springfield, VA 22153, the Harry S. Truman Building and other State Annexes in the Washington, DC area. Additional support may be required at the State Annex 26 in Beltsville, MD and/or the ESOC West Data Center in Denver, Colorado and SA-20 – Rosslyn.

The Government authorizes offeror personnel to telework for the performance of their work functions. If telework or remote work is contemplated for the performance of tasks in this PWS, it shall be conducted per Government telework policies and be authorized by the COR or the CO.

* 1. Period of Performance

This task order comprises a one-year base performance period, with up to four, one-year option periods.

Base Year:

Option Year 1:

Option Year 2

Option Year 3:

Option Year 4

* 1. Standard Work Hours

The Department normal work hours are 8:15 a.m. to 5:00 p.m., Monday through Friday. Contractor personnel are to be available both during normal working hours and as required for after-hours on-call support, when approved in advance by the GTM.

Unless other hours are specified in the task order, hours of performance on the contract will be an 8-hour workday, excluding lunch, but start times may vary depending on the task assignment. The Contractor will be required to cover the core hours from 0900 to 1500, Monday through Friday. During times of emergency and under unusual conditions, i.e. declared emergencies, civil unrest etc., the Contractor shall be prepared for 24-hour performance.

* 1. Security Clearance Requirements

Contractor personnel assigned to this contract shall possess up to a **TOP SECRET** with Special Compartmented Information **(SCI)** personnel security clearance issued by the Defense Counterintelligence and Security Agency (DCSA) commensurate with the level of access required, prior to contract performance. All Contractor personnel supporting this contract will possess at least the minimum-personnel security clearance issued by the Defense Security Service commensurate with the level of access required and as specified in the DD Form 254, prior to contract performance, unless otherwise notified.

Security clearance requirements for contractors accessing DoS information systems shall be in accordance with Volume 12, Foreign Affairs Manual, Section 600. Furthermore, while at DoS locations, the Contractor shall comply with applicable DoS regulations relative to the protection of classified and/or sensitive information. The Office of Information Security (DS/IS/ISP/INB) is responsible for inspecting the Contractor’s activities with at Department locations.

Contractor personnel shall meet the personnel security clearance requirements identified in the DD-254 and task order/s. Most contractor personnel supporting the contract are expected to have a SECRET level security clearance, at a minimum. Additional security clearance requirements may be stipulated by the GTM. The prime or, in the case of a joint venture (JV), the owners of the JV (all primes) must have a TOP SECRET facility clearance by the date of the proposal submission, or it will be considered non-compliant. Subcontractors do need a cleared facility based on the highest-level clearance of their employees.

Visit requests are to be sent to DS/IS/ISP/INB, SA-20, 13th floor, Rosslyn, Virginia 22209. Letters of Consent issued by the Defense Security Service must be attached to all Visit Authorization Requests (VARs). All DD Form 254 for subcontracts shall be forwarded to DS/IS/ISP/INB for certification prior to issuance to the subcontractor.

See the contract clauses and DD 254 for the complete security requirements.

* 1. Non-Disclosure Agreement

The Contractor shall sign a non-disclosure agreement with the Department of State when working with sensitive and/or proprietary information (forms to be executed and maintained by the Contracting Officer Representative (COR)). The Contractor and its employees shall exercise the utmost discretion in regard to all matters relating to their duties and functions. The Contractor shall not communicate to any person any information known to them by reason of their performance of services under this task order which has not been made public, except in the necessary performance of their duties or upon written authorization of the contractor officer.

All documents and records (including photographs) generated during the performance of work under this task order shall be for the sole use of and become the exclusive property of the U.S. Government. Furthermore, no article, book, pamphlet, recording, broadcast, speech, television appearance, film or photograph concerning any aspect of work performed under this task order shall be published or disseminated through any media without prior written authorization of the contracting officer. The contractor shall include the substance of this provision in all contracts of employment and in all subcontracts.

* 1. Organizational Conflict of Interest (OCI)

**Determination:** The Government has determined that this effort may result in an actual or potential conflict of interest or may provide one or more Offerors with the potential to attain an unfair competitive advantage. The nature of the conflict of interest and the limitation on future contracting (description to be included in task order request).

If any such conflict of interest is found to exist, the TO Contracting Officer may (1) disqualify the Offeror, or (2) determine that it is otherwise in the best interest of the United States to contract with the Offeror and include the appropriate provisions to mitigate or avoid such conflict in the task order awarded. After discussion with the Offeror, the TO Contracting Officer may determine that the actual conflict cannot be avoided, neutralized, mitigated or otherwise resolved to the satisfaction of the Government, and the Offeror may be found ineligible for award and if the task order has already been awarded and new information comes to light such as a Corporate Change as described in section f, the government may terminate the contract for connivence.

**Disclosure:** The Offeror hereby represents to the best of its knowledge that:

* + 1. \_\_\_\_It is not aware of any facts which create any actual or potential organizational conflicts of interest relating to the award of this task order, or
    2. \_\_\_\_It has included information in its proposal, providing all current information bearing on the existence of any actual or potential organizational conflicts of interest, and has included the mitigation plan in accordance with paragraph (d) of this provision.

**Mitigation/Waiver:** If an Offeror with a potential or actual conflict of interest or unfair competitive advantage believes it can be mitigated, neutralized, or avoided, the Offeror shall submit a mitigation plan to the Government, IRM/BMP/ITA/CM, for review. Award of a contract where an actual or potential conflict of interest exists shall not occur before Government approval of the mitigation plan. If a mitigation plan is approved, the restrictions of this provision do not apply to the extent defined in the mitigation plan. If not defined, then this provision applies fully.

**Other Relevant Information:** In addition to the mitigation plan, the TO Contracting Officer may require further relevant information from the Offeror. The TO Contracting Officer will use all information submitted by the Offeror, and any other relevant information know to DOS, to determine whether an award to the Offeror may take place, and whether the mitigation plan adequately neutralizes or mitigates the conflict.

**Corporation Change:** The successful Offeror shall inform the TO Contracting Officer and Evolve Program Manager within thirty (30) calendar days of the effective date of any corporate mergers, acquisitions, and/or divestures that may affect this provision.

**Flow-down:** The contractor shall insert the substance of this clause in each first-tier subcontract that exceeds the simplified acquisition threshold.

* 1. Associate Contractor Agreements

Within the first 30 days of task order award the contractor shall provide a draft ACA to the Evolve Program Manager for review and approval. An example is provided in Attachment J-7, Associate Contractor Agreement Sample.

Table in paragraph (g) below will be populated once prime task order contract awardees are known.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(a) The Contractor shall enter into Associate Contractor Agreements (ACA) for any portion of the contract requiring joint participation in the accomplishment of the Government’s requirement. The agreements shall include the basis for sharing information, collected mission requirements, code, data, technical knowledge, expertise, and/or resources essential to the integration of the Evolve

Program and individual task order objectives, software baselines, and components, which shall ensure the greatest degree of cooperation for the development of the program to meet the terms of the contract. Associate contractors are listed in paragraph (g) below.

(b) ACAs shall include the following general information (See template to utilize):

(1) Identify the associate contractors and their relationships.

(2) Identify the program involved and the relevant Government contracts of the associate

contractors.

(3) Describe the associate contractor interfaces by general subject matter.

(4) Specify the categories of information to be exchanged or support to be provided.

(5) Include the expiration date (or event) of the ACA.

(6) Identify potential conflicts between relevant Government contracts and the ACA; include

agreements on protection of proprietary data and restrictions on employees.

(7) Identify the process through which contractors will ensure interoperability of processes and technology used under each task order. For example, ensuring that no tool can only be operated by one contractor

(c) A copy of such agreement shall be provided to the awardees by the Government for review

before execution of the document by the cooperating contractors. All awardees need to collaborate on finalized ACA.

(d) The Contractor is not relieved of any contract requirements or entitled to any adjustments to

the contract terms because of a failure to resolve a disagreement with an associate contractor.

(e) Liability for the improper disclosure of any proprietary data contained in or referenced by any agreement shall rest with the parties to the agreement, and not the Government.

(f) All costs associated with the agreements are included in the negotiated cost of this contract.

Agreements may be amended as required by the Government during the performance of this

contract.

(g) The following contractors are associate contractors with whom agreements are required:

1. Associate Contractors

|  |  |  |
| --- | --- | --- |
| Contractor | Address | Program/Contract |
|  |  |  |
|  |  |  |

* 1. Travel

Personnel assigned to this contract may be required to travel. All officially directed travel, per diem and associated miscellaneous expenses required as a result of work performed under this task order shall strictly adhere to all Government travel regulations. Travel is receipt reimbursable. Unless otherwise specified in the task order, travel to work locations within 50 miles of the National Capital Beltway (495) is considered local travel and will not be reimbursable.

* 1. Other Direct Costs

Other direct costs may be required to deliver the services in this PWS.

* 1. Funding

This task order will be incrementally funded.

1. Task Order Management

Task Order (TO) Management is mandatory for all TOs placed under the Evolve contract. The objective of TO management is to provide the program management, project control and contract administration necessary to manage a high volume, multiple contract type TO process for a large, diversified team so that the cost, schedule and quality requirements of each order are tracked, communicated to the government, and ultimately attained.

The use of commercially available automated tools and the application of expertise on processes and metrics that support task order management are encouraged to achieve the above objectives. The objective of the tool is to provide quicker access, improved accuracy, and enhanced accessibility for Contractors/clients, real-time monitoring of status/deliverables, tracking the quality of work products and gauging overall customer satisfaction.

* 1. Key Personnel

The Contractor shall identify key personnel and provide resumes for these individuals. If the proposed key personnel are not current employees, then the resume must be accompanied with a signed letter of intent that states the prospective employee has authorized their resume to be submitted, intends to accept employment if the Offeror is selected for award, and that the parties have agreed to salary parameters. If any of the key personnel candidates become unavailable at any point during the evaluation process, the Offeror shall immediately notify the Contracting Officer. The contractor shall be able to replace a key personnel within 15 business days. Replacement requires government approval and personnel must meet same criteria as the original employee.

Listed below are minimum key personnel considered essential to the performance of work for this Task Order.

1. Task Order Key Personnel

| Labor Category | **Description** |
| --- | --- |
| Task Order Program Manager | Acts as a single technical point of contact (POC) who shall work closely with the Government Program Manager (PM), Contracting Officer Representative (COR), and Government Technical Monitor (GTM).  The Task Order PM shall:   * Be ultimately responsible for ensuring the Contractor’s performance meets all task order requirements. * Have the requisite authority for full control over all company resources necessary for task order performance. * Have the authority to approve task order modifications in emergent situations. * Be ultimately responsible for personnel management, management of Government material and assets, and personnel and facility security. * Demonstrate progressive IT experience in the functional area of the task order. At least one project shall have occurred within the past three (3) years of similar scope with a total contract value greater than $10M and global delivery in a highly complex environment. Oversight or management of at least one project shall have been conducted in accordance with a CMMI certified, Agile, and ITIL approach. * Demonstrate proven experience and documented success supervising large IT services contracts, including people of various job categories and skills. * Demonstrate expertise in the management and control of costs and resources and demonstrated capability in managing projects of this type and complexity. * Demonstrated experience providing system modernization and innovation that resulted in increased operational efficiency or cost savings.   Minimum qualifications:   * 10 years of relevant experience * Bachelor’s degree in a related field, with a preference for a Master’s degree in Business Administration (MBA) or Information Technology * ITIL Certified, or equivalent * PMP Certified (current), or equivalent * Agile certification highly desired |

* + 1. Substitution of Key Personnel

The Contractor shall notify the TO CO and the TO COR prior to making any changes in Task Order Key Personnel. No changes in TO Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the TO Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The TO CO shall be notified in writing of any proposed substitution at least forty-five (45) days, or sixty (60) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

1. an explanation of the circumstances necessitating the substitution;
2. a complete resume of the proposed substitute; and
3. any other information requested by the TO CO to enable him/her to make a key personnel replacement determination

The Evolve Program Manager and the contract level CO will evaluate substitutions at the contract level and the TO CO and TO COR will evaluate TO level substitutions. Requests will be reviewed promptly the Contractor will receive timely written notification of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days of receipt of the written denial by the Contractor. The Contractor shall allow a minimum of a two-week transition of key personnel.H.11 Insurance

Insurance of the following kinds and minimum amounts shall be furnished at any time at the request of the CO and maintained during the period of performance of this contract:

1. Worker's compensation and employer's liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(a).
2. General liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(b).
3. Automobile liability. The Contractor shall, as a minimum, meet the requirements specified at (FAR) 48 CFR 28.307-2(c).
   1. Meetings/Conferences
      1. Task Order Kick-Off Meeting

The purpose of the Kick-Off Meeting is to achieve a clear and mutual understanding of all task order requirements and to identify and resolve potential problems.

The Contractor shall:

* Attend a task order kick off meeting convened by the Government, onsite or virtual, within 30 days after task order award
* Introduce key personnel during the meeting and present management and risk management processes to be used under the task order, addressing key risks to include dependencies and mitigation for each identified risk
* Update and present the following:
  + - Updated Transition-In Plan
    - Updated Project Management Plan
    - Master Milestone Schedule
    - Associate Contractor Agreement(s)
    - Updated Earned Value Management Plan (if applicable)
    - Agile Reporting Tool (if applicable)

The CO is responsible for establishing the time and place of the conference and will notify the appropriate Government representatives and the Contractors. The Evolve Program Manager will designate or act as the chairperson at the conference. The chairperson of the conference shall conduct the meeting.

The conference may be conducted at a location within the Washington, DC commuting area or completely online at the Government’s discretion.

* + 1. Weekly Operations Meeting

The contractor PM shall convene a weekly operations meeting with the Contracting Officer’s Representative (COR) and other key stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the weekly activities. As part of this meeting, the contractor will prepare a weekly operations report.

The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

* + 1. Monthly Technical Status Meeting

The contractor PM shall convene a monthly Technical Status Meeting with the COR and other key stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and Monthly Program Status Report (MPSR), provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities.

The contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

* 1. Task Order Deliverables

1. Unless the Government identifies otherwise, all deliverables must be submitted in English and in electronic, Microsoft Office compatible, format via email.
2. The Government will review each deliverable product and may provide oral and written comments. The Contractor shall review and incorporate comments or implement directed changes no later than five (5) business days thereafter. This time period may be extended, at the sole discretion of the Government, by written approval of the Contracting Officer or COR (if responsibility has been delegated by the CO).
3. All documentation and reports developed or provided by the Contractor shall become the property of the U.S. Government. Reports shall not contain any markings or legends which will restrict the Department’s use of such reports in any way. All deliverables, including attachments, shall comply with the data right clauses incorporated in the contract. The Government will reject all deliverables containing markings contradicting said clauses.
4. Deliverables longer than 5 pages shall include a table of contents. Attachments, if any, shall include the attachment number, deliverable name and number, and contract number and task order number.
5. For purposes of delivery, all deliverables shall be made by close of business (COB) 4:30 P.M. local time (Washington, DC) at destination, Monday through Friday, unless stated otherwise.
6. All deliverables submitted in electronic format shall be free of any known computer virus or defects. If a virus or defect is found, the deliverable will not be accepted. The replacement file shall be provided within two (2) business days after notification of the presence of a virus.
7. Each deliverable shall be accompanied by a cover letter from the Contractor. Multiple deliverables may be delivered with a single cover letter describing the contents of the complete package.
8. In the event the Contractor anticipates difficulty in complying with any task order-level deliverable, the Contractor shall provide written notification immediately to the task order-level Contracting Officer and TO COR. Each notification shall give pertinent details, including the date by which the Contractor expects to make delivery; PROVIDED, that this data shall be informational only in character and that receipt thereof shall not be construed as a waiver by the Government of any contract delivery schedule, or any rights or remedies provided by law or under this contract.
9. Schedule of Deliverables

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Deliverable | Section Reference | Due Date | Update Frequency | Distribution |
| Associated Contractor Agreement | 3.9 | 30 days after every new task order award and updated as applicable | As needed | Evolve Program Manager |
| Daily Status Report | 4.3.6 |  |  |  |
| Meetings/Conferences (Meeting notes/action items) | 4.2/4.3.5 | 3 working days after meeting / conference | As required | CO, TO COR, Evolve Program Manager |
| Project Management Plan, to include Quality Control Plan | 4.3.3 | Within 30 calendar days after TO award (Draft) | Annually, or upon request |  |
| Task Order Kick Off Meeting (Draft Schedule) | 4.2.1 | Prior to task order start date | N/A |  |
| Task Order Monthly Status Reports | 4.3.4 | 1 month after award of first task order | Monthly | CO, COR, Evolve Program Manager |
| Transition-in Plan | 4.3.1 | 30 calendar days from award of first task order | One-time | TO CO, TO COR, TO CPM |
| Transition-out Plan | 4.3.2 | NLT 120 calendar days prior to the end of contract or 60 calendar days following the Government’s request | One-time | TO CO, TO COR, TO CPM |
| Quality Assurance Surveillance Plan | 4.5.2 |  |  |  |
| Weekly Operations Report | 4.3.7 |  |  |  |

* + 1. Transition-In Plan

The contractor shall develop a Transition-in Plan that details activities that shall be completed no later than 30 calendar days from the effective date of performance.

The Transition-In Plan shall include the following:

* Planned transition activities
* Transition activity timelines and milestones
* Transition resource requirements (includes the retention of current staff, as applicable and appropriate)
* Transition security implications
* Transition risks and mitigation or avoidance strategies; and
* Transition notifications and training of users
  + 1. Transition-Out Plan

The contractor shall develop a Transition-out Plan that facilitates the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the contractor.

The contractor shall provide a final Transition-Out Plan NLT 120 calendar days prior to the end of the contract, or 60 calendar days after the Government requests the deliverable.

The Transition-Out Plan shall include the following:

* Project management processes
* Points of contacts
* Location of technical and project management documentation, data, and methods of providing these to these to the incoming service provider
* Status of ongoing technical initiatives
* Appropriate contractor-to-contractor coordination to ensure a seamless transition
* Transition of Key Personnel
* Schedules and milestones
* Actions required of the Government
* Methods of measuring transition risks that includes a complete inventory of the transition risks, with assigned severity and probability, and response plans to address the risks either through avoidance, mitigation, or other means
* Method of permitting the successor service provider to observe and become familiar with any and all operation specified in this PWS for a minimum of 120 calendar days prior to the expiration or termination of the contract
* Method of establishing and maintaining effective communication with the incoming service provider for the period of the transition via weekly status meetings; and
* Method for ensuring that all information assets and related configuration information is up-to-date and available for the Government’s review at least 120 calendar days prior to the end of the contract
  + 1. Project Management Plan

The Project Management Plan (PMP) shall define policies and procedures for managing and directing the effort for productivity, quality, cost control, and early identification and resolution of problems. The PMP shall include schedules, milestones, tasks, and subtasks required in the PWS.

* The PMP shall provide a Work Breakdown Structure (WBS) or epics with user stories, and associated roles and responsibilities of the Contractor.
* The PMP shall include the Contractor’s Quality Control Plan (QCP), Transition Plan Overview, and the stakeholder management and communication plan. The Contractor shall provide the Government with an initial PMP draft.
* The Contractor will be prepared to review and discuss the initial PMP outline at the Project Kick-Off Meeting. The PMP is a “living document” and shall be updated as necessary to reflect current tasks, objectives, and deliverables. The Contractor shall work from the latest Government approved version of the PMP
  + 1. Task Order Monthly Status Reports (MSR)

The Contractor’s PM shall develop and provide an MSR via electronic mail to the CO, COR and GTM by the 10th of the following month. The Contractor shall consult with the COR on the format of the report. The MSR shall include, at minimum, the following:

* Activities during reporting period, by task (include: on-going activities; new activities; activities completed; progress to date on all above-mentioned activities). Start each section with a brief description of the task
* Problems and corrective actions taken. Also include all new and pending issues or concerns and proposed resolutions to address them
* Personnel gains, losses, and status
* Government actions required
* Project schedule (major tasks, milestones, deliverables, planned and actual start and completion dates, etc.)
* List of all documents submitted during reporting period to include version number and last revision date.
* If applicable, submit a summary of trips taken, conferences attended, etc.

At the CO’s, COR’s, or GTM’s request, a monthly status meeting may be held. In addition, the contractor shall meet as necessary with the government to discuss progress and problems. These meetings shall enable problems to be identified and resolved quickly. The contractor shall document the problems and the solutions.

* + 1. Meeting Minutes

Sharing meeting minutes as a record of information shared at the meeting is a guiding principle for the task order.

All formal meetings’ minutes for staff in an organizational unit shall be shared with Office Directors of the organizational unit at a minimum, either via email or, with the Office Director’s concurrence, a shared online repository. If meetings are informal or non-recurring, then requirements for meeting minutes will be determined by the Government staff in the meeting. Meeting minutes may be shared with additional Government personnel as requested by team leads, Government leadership, and COR/COs. Meeting minutes will only be used for evaluating contract staff if that requirement is coordinated with the COR prior to the start of the meeting and should not be used as a primary performance source.

* + 1. Daily Status Report (SITREP)

The contractor shall submit Daily System/Service Status Report. The Daily System/Service Status Report is an informal means of reporting Customer Support and Mobile Services operations and communicating information about:

* System and service performance.
* Status of current and upcoming events and activities.
* Events that may have an impact on operations.
  + 1. Weekly Operations Report

The contractor shall submit the Weekly Operations (Ops) Report with input from each of the functional areas. The Weekly Operations Report shall provide information about the current state of the operations as well as planned activities.

This report information shall include at a minimum the following sections.

* Service Level Management
* Incidents and Problems
* Changes
* Maintenance
* Projects Status
* Contractual Activities
* Issues
* Other notable areas of concern
  1. Measurements and Reporting

The contractor shall provide performance measurements and reporting for all tasks in the PWS. This not limited to performance measurements detailed in the Performance Summary Table. Data collected will be used to drive data driven decisions at every level of the program.

The contractor shall ensure tasks and activities are captured and measured in the GFE ITSM tool and the performance criteria are correctly annotated in the tool. Dashboards shall be created for each service area. Dashboards shall aggregate data and reports in a logical manner.

Acceptance of all written documents and other deliverables will be contingent upon Government Task Manager (GTM) review and approval. The GTM will discuss each specific task with the Contractor to ensure that the goals and objectives are clearly defined. Required graphs, charts, columns and rows of data shall be legible and properly formatted. Unless valid justification is cited to the contrary, the GTM comments will be incorporated into the respective final documents and reports. If GTM comments given do not conform to safe business practices, or are deemed technically unsound; it is the responsibility of the Contractor to advise the GTM. Consensus is required between the GTM and the Contractor; however if consensus is not achieved, actions will be as directed by the GTM.

Upon approval of the final draft, deliverables will be submitted in final form to the GTM. All deliverables shall be delivered to the GTM in both hard copy and electronic format, which will be determined upon contract award.

* 1. Quality Control and Quality Assurance
     1. Quality Control

The contractor shall develop and maintain an effective quality control program to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, and ensure non-recurrence of defective services. The contractor’s quality control program is the means by which it assures that the work complies with the requirement of the contract.

After acceptance of the quality control plan the contractor shall receive the contracting officer’s acceptance in writing of any proposed change to his QC system.

* + 1. Quality Assurance

The Government will utilize several quality assurance procedures to ensure contractor compliance with this task order, as detailed in attachment J-X: QASP. The QASP sets forth the procedures and guidelines that the Department of State, Bureau of Information Resources Management will use in ensuring the required performance standards or services levels are achieved by the contractor

Examples include inspection of deliverables, review of reports, and onsite progress meetings, performance evaluations, etc. to ensure that, at a minimum, the PWS requirements have been met; sufficient consideration has been given to alternative approaches for implementing the components of the project; and defensible explanations have been provided to justify recommendations, etc.

The contractor shall maintain the highest degree of quality for all activities performed throughout the period of performance of the task order. The Government shall regularly evaluate the Contractor’s performance including, but not limited to:

* Inspections of deliverables identified within this PWS for completeness, accuracy and timeliness; note that it is the Contractor’s responsibility to ensure adherence to the submitted QCP to ensure acceptable performance under the award.
* Assurances that validated and correct implementation strategies have been selected for the program.

The contractors’ ability to retain quality individuals to perform the contact requirementsAppendix A: Basic Performance Standards

The contractor shall meet all the requirements listed in this PWS. Specific minimum performance requirements are listed for defined for tasks in ANNEX I: Customer Support and Mobile Service Performance Requirements Summary in Attachment J-X: QASP. Where specific minimum requirements are not listed, the basic standard is assumed to be an accurate, timely, high-quality product that effectively performs its intended function. The Government may review performance on any and all requirements contained in this PWS. Failure to meet the basic performance standards could result in administrative actions.

### Appendix A: Current Technical Environment

The centralized domestic mobile program supports approximately 46 bureaus throughout the Washington D.C. Metropolitan area, while there are more than 270 overseas posts (See Appendix B for a list of the domestic and international locations). The following profile in the table below is an overview of the mobile devices program.

1. Mobile Device Program Profile

| **Feature** | **Description** |
| --- | --- |
| **Service Geography** | Approximately 334 world-wide locations, 46 domestic and 288 international (see Appendix 7.2 for a list of locations) |
| **Number of Lines\*** | Approximately 50K (approximately 20.5K of domestic and 20.5K international) |
| **Number of Devices\*** | Approximately 50K (approximately 20.5K of domestic and 20.5K international) |
| **Domestic Order Volume and Process** | Approximately 35 per day, including new devices/service and cancelations  Multiple processes and technologies used across the 46 bureaus |
| **Total Annual Spend** | Approximately $20 million annually |
| **Domestic Service / Device Fulfilment** | Third-party Contractor provides: 1) Ordering support for voice, text and data service 2) Ordering support for devices, and 3) Technical support for devices and service |

\*This approximation is a notional value and is provided to give an estimation of scope. This value is subject to change as lines and devices are added and removed.

### Appendix B: Mobile Minimum Technical Requirements

| No. | Requirement | Vulnerability Information | Reference | Additional Information |
| --- | --- | --- | --- | --- |
| 1 | The mobile operating system must prevent modification of key material except during secure, non-operable system states. | Secure, non-operable system states are states in which the information system is not performing mission/business-related processing (e.g., the system is off-line for maintenance, troubleshooting, boot-up, shutdown). If an adversary is able to modify key material, then the adversary may be able to compromise sensitive DoS information. The adversary may also be able to bypass authentication controls on downloaded applications, web sites, and network access points depending on the keys modified. This attack could enable the adversary to install unauthorized applications and stage subsequent attacks on other systems. Preventing modification of key material mitigates the risk of this attack. | NIST SP 800-53, Rev3: AC-3 | Determine if the cryptographic module protecting stored keys is FIPS validated. Review product documentation to determine if there are appropriate controls to protect key material. If available, use scanning tools to determine if keys can be modified by non-privileged users and processes. If such key material can be modified, this is a finding. |
| 2 | The mobile operating system must maintain the binding of digital signatures on software components and applications in storage. | Digital signatures enable the system to verify the integrity of the signed object and authenticate the object's signatory. Failure to maintain the binding of digital signatures on software components and applications in storage makes it more likely that an adversary could modify or replace those objects. Conversely, the bindings enable the operating system to verify the software's integrity and source with a high degree of assurance whenever necessary. | NIST SP 800-53, Rev3: AC-16 | Review system documentation to determine if the operating system maintains the binding of digital signatures to software objects when those objects are stored after installation. If these bindings are not maintained, this is a finding. |
| If the operating system does not support this capability, a permanent finding must be assigned to the asset running the operating system. |
| 3 | The mobile operating system must maintain the binding of digital signatures on software components and applications in process. | Digital signatures enable the system to verify the integrity of the signed object and authenticate the object's signatory. Failure to maintain the binding of digital signatures on software components and applications in process makes it more likely that an adversary could modify or replace those objects when the software is executed. The bindings enable the operating system to verify the software's integrity and source just before the execution process. | NIST SP 800-53, Rev3: AC-16 | Review system documentation to determine if the operating system maintains the binding of digital signatures to software objects when those objects are stored after installation. If these bindings are not maintained, this is a finding. |
| If the operating system does not support this capability, a permanent finding must be assigned to the asset running the operating system. |
| 4 | The mobile operating system must use cryptography to protect the confidentiality of remote access sessions. | Remote network access is accomplished by leveraging common communication protocols to establish a remote connection. These connections typically will occur over the public Internet. Without cryptographic protection, sensitive DoS information could be captured by an adversary with access to the infrastructure used to support the remote access session. Using cryptography provides assurance that the content of remote access sessions will remain confidential. | NIST SP 800-53, Rev3: AC-17 (2) | Review product documentation to verify cryptography is used to protect the confidentiality of remote access sessions. If there is doubt about claims in the documentation, use a network protocol analyzer to verify data in remote access sessions are encrypted. If it is determined that cryptography does not protect the confidentiality of remote access sessions, this is a finding. |
| 5 | The mobile operating system must log an audit event for each instance when a remote process uses MDM mechanisms for accessing the device security configuration settings. | An MDM provides security services to mobile devices but it also represents a threat to those devices. If an adversary were able to take control of the MDM or masquerade as the MDM, then it could use that ability to relax security controls and breach the mobile device. Logging MDM events enables better traceability to mistaken or unauthorized MDM transactions. | NIST SP 800-53, Rev3: AC-17 (7) | Use the MDM to perform a temporary and relatively innocuous security configuration change on a small sample of devices. Verify the operating system logged this event. If there is a not an audit entry for this event, this is a finding. |
| 6 | The mobile operating system must disable the capability for automatic installation and execution of applications on the device without user direction. | If the applications can be installed or executed without user (or mobile device management) direction, then these applications may be used to access sensitive information or otherwise compromise system integrity to launch subsequent attacks. Requiring that the user take an action to permit the installation and execution of an application makes it more likely that malware will be identified and kept off of mobile devices. | NIST SP 800-53, Rev3: AC-19 | Review the operating system configuration to determine if this capability is disabled. If this capability is not configurable, review product documentation and security information resources to determine whether automatic installation of applications without user direction is feasible. If applications are able to either install or execute without user direction, this is a finding. |
| 7 | The mobile operating system must enforce a password-based lock feature in which the device may only be unlocked upon entry of the correct password. | If the operating system does not enforce a lock feature, then anyone who gains access to the device when it is not in the user's possession may be able to access sensitive DoS information or perform other authorized functions. The lock features mitigates the risk of unauthorized access. | NIST SP 800-53, Rev3: AC-11 b | Inspect a device running the operating system to ensure it enforces a lock feature. If a lock feature is not present, this is a finding. |
| 8 | The mobile operating system must lock the device after no more than 15 minutes of inactivity. | If a device remains unlocked after a significant period of inactivity, there is risk that it is unattended and is vulnerable to breach from an authorized individual. In this case, anyone can simply pick up the device and have access to information on the device and the networks to which the device is connected. An automatic lock after a period of inactivity reduces the period in which this attack would be successful. | NIST SP 800-53, Rev3: AC-11 a | Examine the operating system to verify the inactivity time period is no more than 15 minutes. If the time period has not been set to 15 minutes or less, or if the capability is not configurable, this is a finding. |
| 9 | The mobile operating system must permit the device's user to lock the device at any time. | If the user does not have the ability to lock the device when the user determines it necessary (e.g., the device will temporarily be outside of the user's possession), then an adversary who gains possession of the device may have access to that user's data and applications. | NIST SP 800-53, Rev3: AC-11 a | Inspect a device running the operating system to determine if it supports a lock feature that the user can activate. |
| 10 | The mobile operating system session lock mechanism, when activated on a device, must place a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen. | If the device still displays user information when the device is locked, that information will be visible to anyone in possession of the device. If the information is sensitive, then this would result in compromise of sensitive information. Hiding user information when the phone is locked mitigates this risk. | NIST SP 800-53, Rev3: AC-11 (1) | Lock a device running the operating system and verify the display hides what was previously visible when the device was in an unlocked state. If any portion of the user display remains, even if it does not reveal data, this is a finding. |
| 11 | The mobile operating system must disable access to the device's contact database when the device is locked. | On some devices, users can access the device's contact database to obtain phone numbers and other information using voice-activated Bluetooth peripherals even when the phone is locked. Often this information is personal identifying information (PII), which is considered sensitive. It could also be used by an adversary to profile the user or engage in social engineering to obtain further information from other unsuspecting users. Disabling access to the contact database in these situations mitigates the risk of this attack. Exceptions to this requirement must be evaluated and authorized on a case by case basis if the operational environment requires this capability. | NIST SP 800-53, Rev3: AC-14 a | Review system documentation and operating system configuration to determine the ways in which someone can access the contact database, focusing on ways to so without viewing the display (e.g., voice commands or Bluetooth peripherals). If there are no such methods, there is no finding. If there are such methods, verify the effectiveness of the control. On a sample device, view the contact database and select a couple of entries. Lock the phone and then try to access the contact database using the identified methods. If you can access the data, this is a finding, unless the DAA has issued a written waiver. |
| 12 | The mobile operating system must enable a system administrator to select which data fields will be available to applications outside of the contact database application. | The contact database often contains a significant amount of information beyond each person's name and phone number. The records may contain addresses and other identifying or sensitive information that should not be revealed. There may be cases in which an organization has determined that it is an acceptable risk to distribute parts of person's contact record but not others. Enabling the system administrator to select which fields are available outside the contact database application assists with management of the risk. | NIST SP 800-53, Rev3: AC-14 a | Review system documentation to determine if this capability is present. If it is not, this is a finding. If the capability is alleged to be present, ask the systems administrator to disable access to one of the fields in the contact database (e.g., organization name). This may be accomplished using an MDM system. Find an application that can access the contact database and verify the blocked field is inaccessible. If it is accessible, this is a finding. |
| 13 | The operating system must dynamically reconfigure security attributes in accordance with an identified security policy as information is created and combined. | Security attributes are abstractions representing the basic properties or characteristics of an entity (e.g., subjects, objects) with respect to safeguarding information. These attributes are typically associated with internal data structures (e.g., data records, buffers, files) within the application and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy. | NIST SP 800-53, Rev3: AC-16 (1) | Verify security settings dynamically change according to MDM settings. If the settings do not change as expected, this is a finding. |
| (Note: This requirement is contingent on the capabilities of MDM. It would be great to be able to dynamically configure a device based on location and connection) |
| 14 | The mobile operating system must display to the user the identity of the entity that signed a downloaded application before installing the application. | The user provides an important line of defense in protecting the system against the installation of malicious software. It is more likely that software will be installed from unknown sources if the user is unaware of the transactions. Revealing the signatory of downloaded software to the user enables the user to identify rogue or suspect sources prior to installation, and possibly abort the transaction or report the concern to the IAO. | NIST SP 800-53, Rev3: AC-16 (5) | On a sample of devices, download an application and verify the operating system reports the signatory of the application to the user. If the operating system does not display such a message, this is a finding. |
| 15 | The mobile operating system must display to the user the operating system permissions that a downloaded application is requesting before installing the application. | The user provides an important line of defense in protecting the system against the installation of malicious software. It is more likely that software will obtain greater permissions than necessary if the user is unaware of permissions that the application is seeking. Revealing to the user the permissions that the application will be granted enables the user to identify suspect behavior sources prior to installation and possibly abort the transaction or report the concern to the IAO. | NIST SP 800-53, Rev3: AC-16 (5) | On a sample of devices, download an application and verify the operating system displays to the user the permissions that the application is requesting prior to installation of the application. If the operating system does not display such a message, this is a finding. |
| 16 | The mobile operating system must display to the user the identity of the entity that signed a downloaded application upon user request. | The user provides an important line of defense in protecting the system against the installation of malicious software. It is more likely that unauthorized software will remain resident on a system if the user (or a systems administrator) is unaware of the source of the software. Revealing to the user the signatory of the application enables the user (or systems administrator) to evaluate whether the source is authorized. | NIST SP 800-53, Rev3: AC-16 (5) | On a sample of devices, determine if a user can determine the signatory of the application on request. The operating system should display this information to the user. If the operating system does not display such a message, this is a finding. |
| 17 | The mobile operating system must display to the user the operating system permissions that a downloaded application has been granted upon user request. | The user provides an important line of defense in protecting the system against the installation of malicious software. It is more likely that software will obtain greater permissions than necessary if the user is unaware of permissions that the application has been granted. Revealing to the user the permissions that the application has been granted enables the user to identify excess permissions whenever the user suspects that an application is exhibiting unauthorized behavior. The user then can report this information to a system administrator or IAO. | NIST SP 800-53, Rev3: AC-16 (5) | On a sample of devices, determine if a user can determine what the permissions or entitlement of query the device to determine if it downloaded an application and verify the operating system displays to the user the permissions that the application is requesting prior to installation of the application. If the operating system does not display such a message, this is a finding. |
| 18 | The mobile operating system must not execute software programs embedded in data files (e.g., executables in PDF, adware, etc.). | If the operating system or a resident software application executes code contained in data files, the code will likely run with the same privileges as the operating system or application that launched it. If the code is malicious, this may give an adversary the ability to compromise sensitive DoS information or install additional capabilities that would enable further attacks. If the operating system does not execute software programs embedded in data files, this mitigates the risk of this attack. | NIST SP 800-53, Rev3: AC-4 (5) | Review product documentation or security information resources to determine if the operating system supports the capability to execute code embedded in data files. If the operating system permits configuration of this feature, check that the capability is disabled. If the feature is not disabled, or if the operating system permits such execution by default, this is a finding. |
| 19 | The mobile operating system must notify the MDM of certificate failures related to digital signatures on software applications or components. | A certificate failure related to a digital signature on software applications or components is strong evidence of a system breach. Notifying the MDM of such an occurrence allows the enterprise to assess the situation, contain the breach if there is one, and possibly invoke incident response procedures. | NIST SP 800-53, Rev3: AC-4 (17) (c) | Review system documentation and operating system configuration to determine if this capability is present. If additional assurance of compliance is needed, attempt to download an application with a known bad certificate and determine if the operating system notifies the MDM of the failure. This test may require the placement of a test application with an invalid signature in the online mobile application store. If the operating system does not verify digital signatures, does not verify them correctly, or does not notify the MDM of such failures, this is a finding. |
| 20 | The mobile operating system must notify the user of certificate failures related to digital signatures on software applications or components. | A certificate failure related to a digital signature on software applications or components is strong evidence of a system breach. Notifying the user of such an occurrence allows the user to notify the user's technical support personnel and IAO, as well as proceed with caution regarding activities performed on the device. If the operating system does not notify the user of certificate failures related to digital signatures on software applications or components, this is a finding. | NIST SP 800-53, Rev3: AC-4 (17) (c) | Review system documentation and operating system configuration to determine if this capability is present. If additional assurance of compliance is needed, attempt to download an application with a known bad certificate and determine if the operating system notifies the user of the failure. This test may require the placement of a test application with an invalid signature in the online mobile application store. |
| 21 | The mobile operating system must not permit an application to perform functions not included in its manifest. | An important aspect of security on mobile devices is preventing applications from performing functions that they were not intended to perform. Mobile operating systems may implement this control through permissions or entitlements listed in a manifest attached to the application, or through some similar mechanism. If an the operating system permits an application to perform functions not delineated in the manifest, this might allow the application to access sensitive information or otherwise breach system security. Limiting applications to the functions delineated in the manifest reduces the risk of unauthorized behavior. | NIST SP 800-53, Rev3: AC-4 | Using a jailbreak or root detection tool or MDM solution, verify applications cannot perform functions for which permissions were not delineated in the manifest. If any application is able to bypass the manifest permission or entitlement control, this is a finding. |
| 22 | The mobile operating system must not permit a user to disable the password-protected lock feature on the device. | If the user is able to disable the password-protected lock feature, the user can change the configuration of the device to allow access without a password. The modified configuration would enable an adversary with access to the device to obtain DoS information and possibly other information resources on other systems. An operating system that does not allow a user to disable this feature mitigates the risk of this attack. In cases in which the mobile operating system relies on another application for protected data storage (e.g., if FIPS-validated encryption is not native to the device), then this requirement applies to both the device lock password and the password to the data storage application. | NIST SP 800-53, Rev3: AC-6 | Review the operating system configuration to determine if there is a configuration option for the user to disable the password lock feature. If such a configuration option is present, this is a finding. |
| 23 | The mobile operating system must not permit a user to disable or modify the security policy or enforcement mechanisms on the device. | The integrity of the security policy and enforcement mechanisms is critical to the security posture of the operating system. If a user can modify a device's security policy or enforcement mechanisms, then a wide range of subsequent attacks are possible, including unauthorized access to information and networks. Access controls that prevent a user from making modifications such as these mitigate the risk of operating system compromise. | NIST SP 800-53, Rev3: AC-6 | Review system documentation, operating system configuration, and other security information resources to determine how the operating system prevents the user from modifying the security policy and related enforcement mechanisms. Items to look for include mandatory access controls, permissions on related operating system files, and authentication for super user access. Examine the operating system configuration. If it is easy to turn off security settings or stop security-related applications from running, this is a finding. If the documentation reveals other means of achieving these ends, this is also a finding. |
| 24 | The mobile operating system must wipe all storage media after an organization defined number of consecutive, unsuccessful attempts to unlock the mobile device. | Mobile devices present additional risks related to attempted unauthorized access. If they are lost, stolen, or misplaced, attempts can be made to unlock the device by guessing the password. Once unlocked, an adversary may be able to obtain sensitive data on the device. Wiping storage media renders all such data permanently inaccessible. There are two acceptable methods to wipe the device. The first is to overwrite the data on the media several times, so it is no longer recoverable. In this case, the device should implement a wipe (3pass), in which the media is overwritten three times. The second is to delete the locally stored encryption key on a device that encrypts all data stored on the device. In this case, the key must be wiped using a method complying with a higher standard of wipe (7 pass), in which all storage sectors containing the key are overwritten seven times. | NIST SP 800-53, Rev3: AC-7 | Review system documentation and operating system configuration to determine if the system wipes all storage media after an organization defined number of consecutive, unsuccessful attempts to unlock the mobile device. Check if the chosen wipe method uses at least three passes for data and at least 7 passes for keys. If feasible, on a spare device, test if the control is enforced by entering the requisite number of incorrect passwords. The device should be inoperable after the wipe process. If the system is not configured for the device wipe functionality, this is a finding. |
| 25 | The mobile operating system must wipe data on both embedded and removable memory when performing a data wipe function. | Sensitive data may be resident on both embedded and removable memory. If the operating system only performs the wipe function on one type of memory, then this will leave the other vulnerable. Ensuring the wipe occurs on both embedded and removable memory mitigates this risk. | NIST SP 800-53, Rev3: AC-7 (2) | Review system documentation and operating system configuration to determine if mobile operating system wipes data on both embedded and removable memory when performing a data wipe function. If feasible, on a spare device, test that the control is enforced by entering the requisite number of incorrect passwords. If the system is not configured to wipe both embedded and removable memory, this is a finding. |
| 26 | The maximum number of consecutive unsuccessful unlock attempts must be configurable within a range from 3 to 10. | The recommended setting for the maximum number of consecutive unsuccessful unlocks attempts is 10. In some environments, a lower number may be needed to provide greater protection of sensitive information. Allowing for configuration enables the local command to enforce greater protection when it is deemed necessary. If the limit is not configurable, then it is permissible for a site to procure and deploy devices that enforce the limit, so long as that limit does not exceed 10. | NIST SP 800-53, Rev3: AC-7 (2) | Review system documentation and operating system configuration to determine if the maximum number of consecutive unsuccessful unlocks attempts is configurable within a range from 3 to 10. If this operating system parameter is not configurable, check that the operating system nonetheless supports the limit specified by the organization, which is an acceptable alternative. If the limit is not configurable and is not compliant with the organization defined limit or the limit exceeds 10, this is a finding. |
| 27 | The mobile operating system must display the DoS warning banner exactly as specified before or immediately after device unlock. | The operating system is required to display the DoS approved system use notification message or banner before granting access to the system. This ensures all the legal requirements are met as far as auditing and monitoring are concerned. The banner must read "I've read & consent to terms in IS user agreement." If this banner is implemented, the requirement is satisfied. | NIST SP 800-53, Rev3: AC-8 (a) | Inspect a sample of devices to ensure they display the correct banner text: "I've read & consent to terms in the mobile device user agreement." If the operating system is not capable of supporting a banner before or immediately after device unlock, then this is a finding. If there is no banner, or if the banner's wording does not match the approved wording, this is a finding. |
|  |
| Banner text: "I've read & consent to terms in the mobile device user agreement." |
| 28 | The mobile operating system, before or upon successful unlock, must display to the user the number of unsuccessful unlock attempts since the last successful unlock. | Users need to be aware of activity that occurs regarding their account. Providing users with information regarding the number of unsuccessful attempts that were made to login to their account allows the user to determine if any unauthorized activity has occurred and gives them an opportunity to notify administrators. | NIST SP 800-53, Rev3: AC-9 (1) | On a sample of devices, attempt to unlock the device with improper authentication credentials. Then have the user successfully unlock the device. Inspect the device to determine if it displays the number of unsuccessful unlock attempts since the last successful unlock. Vary the number of attempts on the sampled devices to determine if the operating system correctly identifies the number of unsuccessful attempts, taking care not to exceed the maximum number of unsuccessful attempts before the operating system forces a wipe of the device. If the operating system does not display to the user the number of unsuccessful unlock attempts, this is a finding. |
| 29 | The mobile operating system must notify the user of the number of unsuccessful unlock attempts that have occurred since the device was last locked or shut down. | If a user is informed of the number of unsuccessful unlock attempts that have occurred since the device was last locked or shut down, the user can use this information to assess whether another individual is trying to obtain access to features on this device, and can report the attempts to security personnel. | NIST SP 800-53, Rev3: AC-9 (2) | On a sample of devices, attempt to log on using an invalid password. On the next attempt, verify the operating system reports information on the first invalid attempt. If the device does not report such invalid attempts, this is a finding. |
| 30 | The mobile operating system must validate the digital signature on signed software components or applications. | Digital signatures on software components and applications are primary means to determine that the code comes from a trusted source and has not been modified. If the operating system does not validate these digital signatures, then there is the potential for malware to infiltrate the device. Validating digital signatures assures that the digital signature control properly mitigates the risk that malware will be installed or execute on the system. | NIST SP 800-53, Rev3: AU-10 (2) | Review system documentation and operating system configuration to determine if the digital signatures on software components and applications are being validated. If higher assurance is required, provide the operating system with a software application that has an invalid signature to verify the operating system can detect the invalid signature. If the system fails this test or documentation or configuration shows that the capability is not present, this is a finding. |
| 31 | The mobile operating system must generate audit records for the DoS-required auditable events. | The DoS-required auditable events are events that assist in intrusion detection and forensic analysis. Failure to capture them increases the likelihood that an adversary can breach the system without detection. | NIST SP 800-53, Rev3: AU-12 c | Review product documentation and the system configuration to determine if the DoS-required auditable events are recorded. |
|  |
| Required events include: system startup and shutdown, successful and unsuccessful device unlock attempts, program execution, integrity validation failures, Internet activity (e.g. browser history, uploaded files). |
| Verify a reasonable subset of these events is captured in practice by examining the audit logs. If it is apparent that the audit logs do not include DoS-required auditable events, this is a finding. |
| 32 | The operating system must initiate security auditing at system start-up. | The audit capability is most effective if it is running at all times. Otherwise there may be time gaps in the audit logs in which an adversary can hide malicious behavior. Initiating security auditing at system start-up mitigates the risk that there will be time periods in which auditing is not active. | NIST SP 800-53, Rev3: AU-14 (1) | On a sample of devices, restart the device. Immediately after the boot process is complete, verify auditing has been initiated. Access to the audit logs may only be possible through an MDM. If security auditing is not operational after system start-up, this is a finding. |
| 33 | The mobile operating system must produce audit records containing the severity level of each recorded event. | Operating system auditing capability is critical for accurate forensic analysis. Event severity levels allow system administrators and security personnel to more easily identify critical system issues and debug software. | NIST SP 800-53, Rev3: AU-3 | On a sample of devices, review the audit logs to determine if they contain entries with the severity level of each recorded event. If any event in the log does not have an event severity level, this is a finding. |
| 34 | The mobile operating system must include date and timestamps (to one second resolution) in each event recorded in audit logs. | Operating system auditing capability is critical for accurate forensic analysis. The inclusion of timestamps better enables for correlation of events across disparate systems, which can be critical to isolating security incidents and developing appropriate countermeasures. | NIST SP 800-53, Rev3: AU-3 | On a sample of devices, review the audit logs to determine if the entries have timestamps with a resolution of at least one second (i.e., the entry shows the second it occurred). If any log entry does not have a timestamp with a resolution of at least one second, this is a finding. |
| 35 | The mobile operating system must include the software component (e.g., hardware drive, user application, or operating system security module) that generated each event recorded in audit logs. | Operating system auditing capability is critical for accurate forensic analysis. The inclusion of software component that generated each even in the audit logs enables system administrators and security personnel to identify the source of problems and incidents. | NIST SP 800-53, Rev3: AU-3 | On a sample of devices, review the audit logs to determine if the entries include the software component that generated the event. If an entry does not provide information regarding the source of the event, this is a finding. |
| 36 | The mobile operating system must support the transfer of audit logs to remote log or management servers. | Operating system auditing capability is critical for accurate forensic analysis. The ability to transfer audit logs often is necessary to quickly isolate them, protect their integrity, and analyze their contents. | NIST SP 800-53, Rev3: AU-3 (2) | Verify the audit logs can be transferred from the mobile device to a storage location other than the device itself. The systems administrator of the device may demonstrate this capability using a mobile device management server or other means. If audit logs cannot be transferred on request or on a period schedule, this is a finding. |
| 37 | The mobile operating system must allocate sufficient audit record storage capacity for 24 hours of operation. | Operating system auditing capability is critical for accurate forensic analysis. Without adequate storage for audit records, there is the potential that critical audit records will be lost or overwritten. An adversary may be able to take advantage of lack of audit storage capacity to avoid detection. Allocating sufficient audit record storage capacity for 24 hours allows the device to capture critical events even if it is unable to reach the MDM for a full day, such as when an employee may be temporarily in a remote location. | NIST SP 800-53, Rev3: AU-4 | On a sample of devices, review the audit logs for several days to determine the storage used for the entries on the day with the greatest audit log activity. The logs may need to be ported to another device to parse and measure the entries for each day. Make sure that the reserved audit capacity is greater than the log size for the day with the greatest log activity. It is advised that the allocated storage capacity be at least 150% of that needed for the most active day observed. Also use other available information resources (e.g., vendor documentation) to determine appropriate required capability based on industry norms. If the reserved storage for the audit records is less than indicated by these guidelines, this is a finding. |
| 38 | The mobile operating system must send alerts to the MDM when the audit log size reaches an organization defined critical percentage of capacity and full capacity. | Operating system auditing capability is critical for accurate forensic analysis. Alerting administrators when audit log size thresholds are exceeded helps ensure the administrators can respond to heavy activity in a timely manner. Failure to alert increases the probability that an adversary's actions will go undetected. | NIST SP 800-53, Rev3: AU-4 | Verify the alert capability is configured appropriately on the operating system. Also verify the MDM receives the alerts. If the alert capability is not configured, is configured improperly, or the MDM does not receive the alerts, this is a finding. |
| 39 | The mobile operating system must overwrite the oldest audit log entries when audit logs reach capacity. | It is critical that when a system is at risk of failing to process audit logs as required, it detects and takes action to mitigate the failure. Overwriting the oldest audit log entries is the safest course of action in the context of the limited resources available on a mobile device that may not have network connectivity. | NIST SP 800-53, Rev3: AU-5 b | Review the configuration settings to determine if the audit system is configured to overwrite the oldest audit log entries when audit logs reach capacity. If this capability is not apparent from the configuration files or vendor documentation, then take actions to fill the audit logs and verify the oldest entries are overwritten when the log is full. If the oldest entries are not overwritten, this is a finding. |
| 40 | The mobile operating system must use internal system clocks to generate timestamps for audit records. | Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. The internal system clock is an acceptable source to ensure consistency of time across functions that use time to generate audit records. | NIST SP 800-53, Rev3: AU-8 | If the system uses configuration files for this capability, review the system configuration files to determine if the internal system clock is used for timestamps. If this is not feasible, an alternative workaround is to take an action that generates an entry in the audit log and then immediately query the operating system for the current time. A reasonable match between the two times will suffice as evidence that the system is using the internal clock for timestamps. If it is apparent that the operating system does not use the internal system clock to generate timestamps, this is a finding. |
| 41 | The mobile operating system must synchronize internal information system clocks with DoS approved time servers at least once every 24 hours. | Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events. Periodically synchronizing internal clocks with an authoritative time source helps ensure time is synchronized across the enterprise. The USNO time servers provide accurate time and are recommended. This synchronization facilitates event correlation and increases the likelihood that the scope and severity of a security incident will be fully understood, thereby enabling an effective response to the incident. | NIST SP 800-53, Rev3: AU-8 (1) | If the system uses configuration files for this capability, review the system configuration files to determine if the operating system synchronizes its clock to an authoritative time source. Verify the configured authoritative time sources are the ones intended. The USNO time servers and are recommended, but if they are not available in the environment in which the device is used, then other DoS approved time servers are acceptable. If the system relies on any non-DoS approved source for time, this is a finding. |
| 42 | The mobile operating system must protect the confidentiality of the provisioning data downloaded to the handheld device during a trusted over-the-air (OTA) provisioning session. | Provisioning data may be sensitive and therefore must be adequately protected. An adversary within the general proximity of the mobile device can eavesdrop on OTA transactions, making them particularly vulnerable to attack if confidentiality protections are not in place. Proper use of cryptography provides strong assurance that provisioning data is protected against confidentiality attacks. | NIST SP 800-53, Rev3: CM-5 | Review system documentation and operating system configuration to determine if there is appropriate cryptography protecting the confidentiality of OTA provisioning. If the provisioning data is not protected by cryptographic means during an OTA provisioning procedure, this is a finding. |
| 43 | The mobile operating system must protect the integrity of the provisioning data downloaded to the handheld device during a trusted over-the-air (OTA) provisioning session. | Provisioning data may be sensitive and therefore must be adequately protected. It may be possible for an adversary within the general proximity of the mobile device to hijack provisioning sessions and modify data transmitted during the provisioning process. Proper use of cryptography provides strong assurance that provisioning data is protected against integrity attacks. | NIST SP 800-53, Rev3: CM-5 | Review system documentation and operating system configuration to determine if there are appropriate integrity mechanisms protecting the confidentiality of OTA provisioning. Appropriate integrity mechanisms generally involve the use of FIPS validated cryptographic modules implementing algorithms that provide integrity services. If there are no such mechanisms present, this is a finding. |
| 44 | The mobile operating system must support the capability for the system administrator to disable over-the-air (OTA) provisioning. | In some environments, the risk of OTA provisioning may outweigh any convenience benefit it offers. In such cases, the administrator should have the ability to disable OTA provisioning to ensure secure breaches do not occur from use of this technique. | NIST SP 800-53, Rev3: CM-5 | Review system documentation and operating system configuration to determine if the system administrator has the ability to disable OTA provisioning. If the operating system does not support OTA provisioning, this also meets the requirement. If the operating system supports OTA but there is no means for the SA to disable that capability, this is a finding. |
| 45 | A trusted loading process must be the foundation for installation of the mobile operating system and applications on the device during provisioning (whether tethered or over-the-air). | When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. A trusted loading process includes access restrictions pertaining to change control. | NIST SP 800-53, Rev3: CM-5 | Review the loading process to determine if it meets the necessary assurance criteria to be considered trusted. If the trusted loading process does not meet the criteria, this is a finding. |
| 46 | The mobile operating system must provide mutual authentication between the provisioning server and the provisioned device during a trusted over-the-air (OTA) provisioning session. | When dealing with access restrictions pertaining to change control, it should be noted that any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Mutual authentication ensures both that the device is authorized for provisioning and that a rogue provisioning server is not used to obtain software. | NIST SP 800-53, Rev3: CM-5 | Review system documentation and operating system configuration to determine if there is mutual authentication between the provisioning server and the provisioned device. If additional assurance is required, validate the provisioning server will not provision software and data to an unauthorized device and that an authorized device will not connect to an unauthorized provisioning server (e.g., a valid provisioning server with its credentials temporarily removed for the test). If either the device does not authenticate the provisioning infrastructure, or vice versa, this is a finding. |
| 47 | The mobile operating system must record an event in the device audit log each time the device operating system is started. | Some operating system features, including security enforcement, may only be modified when the operating system is not running. Logging startup events provides valuable information on system problems and potential OS integrity issues. | NIST SP 800-53, Rev3: CM-5 (1) | Inspect the audit logs to determine whether startup events are being recorded. Restart the device and check that this occurrence was recorded in the audit log. If a startup event does not appear in the log, this is a finding. |
| 48 | The mobile operating system must record an event in the device audit log each time the user or MDM makes a security relevant configuration change. | Any changes to the hardware, software, and/or firmware components of the information system and/or application can potentially have significant effects on the overall security of the system. Security relevant configuration changes, if not authorized, is a breach of system security and might indicate a broader security attack is occurring. Recording security relevant changes in the audit logs mitigates the risk that unauthorized changes will go undetected. | NIST SP 800-53, Rev3: CM-5 (1) | Inspect the audit logs to determine whether security relevant configuration changes are being recorded. Make several security relevant configuration changes and verify these were recorded in the audit log. If any of the security relevant changes does not appear in the log, this is a finding. |
| 49 | The mobile operating system must prevent the installation of applications that are not digitally signed with an organizationally accepted private key. | Any changes to the hardware, software, and/or firmware components of the information system and/or application can potentially have significant effects on the overall security of the system. Digital signatures on code provide assurance that the code comes from a known source and has not been modified. | NIST SP 800-53, Rev3: CM-5 (3) | Review system documentation and operating system configuration to determine if the operating system prevents the installation of applications that are not digitally signed with an organizationally accepted private key. If greater assurance of compliance is required, attempt to install an application that is not signed with an organizationally accepted private key and verify the operating system blocks this from occurring. Depending on the device's configuration, this procedure may require posting an unsigned or improperly signed test application on an approved application download server. If the operating system does not prevent the installation of applications that are not digitally signed with an organizationally accepted private key, this is a finding. |
| 50 | The mobile operating system must disable the device upon the MDM agent's instruction. | Under some conditions, a compromised device represents a threat to other computing resources on the network. For example, a compromised device may attempt to conduct a denial of service attack on other devices, or may be executing a mechanism to spread malware before a countermeasure has been put in place. In these situations, it is critical that an MDM be able to disable the device to protect other network resources. This enables a system administrator to perform the wipe remotely when circumstances warrant this level of protection. | NIST SP 800-53, Rev3: CM-5 (7) | Identify a sample device that is not required for operational support. Verify it is able to access the network. Then ask the MDM administrator to disable the device from the MDM, and verify the device is no longer operational. If the site does not have a sample device available, the site may provide log evidence that a device had been disabled in the past in lieu of a live test of the capability. If the site cannot provide evidence of the MDM capability to disable a device, this is a finding. |
| 51 | The mobile operating system must employ the capability of a Mobile Device Manager (MDM) to centrally manage configuration settings, including security policies. | Security related parameters are those parameters impacting the security state of the system and include parameters related to the implementation of other security controls. If these controls are not implemented, the system may be vulnerable to a variety of attacks. The use of an MDM allows an organization to assign values to security related parameters across all the devices it manages. This provides assurance that the required mobile OS security controls are being enforced, and that the device user or an adversary has not modified or disabled the controls. It also greatly increases efficiency and manageability of devices in a large scale environment relative to an environment in which each device must be configured separately. | NIST SP 800-53, Rev3: CM-6 (1) | Inspect a sample of mobile devices and the MDM to verify the MDM is being used to centrally manage the devices. Ask a system administrator to push a temporary configuration setting to one of the devices to validate the MDM configuration capability is operational. |
|  |
| The mobile OS must support the ability of an MDM to enable or disable the following device interfaces: |
| Wi-fi Radio, Bluetooth Radio, NFC, GPS receiver, Near-field communications radio, Infrared port, Microphone, Camera, Memory Cardport and USB port. |
| The mobile OS must further support the ability of an MDM to restrict how these interfaces are used when they are enabled. Required managed functions include the ability to enable or disable: |
| Over the air provisoning; Wi-Fi tethering; NFC; Automatic connection to known Wi-Fi sites; Presonal hotspot functionality; -Bluetooth profiles other than the serial port, headset, hands free, or phone book profiles;Bluetooth discoverable mode; VPN split tunneling functionality; Audio recording functionality; Video recording functionality; Location services; Short message service (SMS); Multimedia messaging service (MMS); USB mass storage mode; Availability of contact database information when device is locked; and Contact database fields available outside the contact application. |
|  |
| The mobile OS also must support the ability of an MDM to enforce the following security related configuration parameters: Device unlock password; Device unlock password complexity; Duration of inactivity before device lock; Encryption of data on storage media; Encryption of data in transit; Permitted applications (application whitelist); Prohibited web sites (web site blacklist); and |
| Web proxy URL. |
|  |
| Finally, the mobile operating system must support the ability of the MDM agent application to scan the device at a periodic interval configured on the agent, and initiate commands to wipe storage media. |
| If the MDM is not capable of managing any of the required settings listed above, this is a finding. |
| 52 | The mobile operating system must disable Bluetooth discoverable mode upon a system administrator or MDM agent's instruction to do so. | When a Bluetooth device is in discoverable mode, other devices can discover it and potentially pair with it. Once devices are paired, the remote device may be able to obtain DoS data or otherwise compromise the operating system. To mitigate the risk of this attack, devices should only be in discoverable mode for the brief period necessary to pair with an authorized device. It should be disabled at all other times. | NIST SP 800-53, Rev3: CM-6 (1) | Review system documentation and operating system configuration to determine how and when the device enables and disables Bluetooth discoverable mode. Verify the device will not pair with another Bluetooth device when discoverable mode is off. If Bluetooth discoverable mode is active at any other time other than required for a pairing operation, this is a finding. |
| 53 | The mobile operating system must disable the Bluetooth protocol stack. | All active wireless interfaces on a device pose a potential vulnerability to the system. An adversary may learn of new vulnerabilities in communications protocols or in the implementation of those protocols for which the system does not have defenses. If an organization has reason to believe that the Bluetooth stack is vulnerable, or learns of a vulnerability that cannot be immediately corrected, then disabling the Bluetooth stack is an effective means to mitigate the risk. | NIST SP 800-53, Rev3: CM-6 (1) | Review system documentation and operating system documentation to determine if a systems administrator can disable the Bluetooth protocol stack. The system administrator may accomplish this functionality using an MDM. If a systems administrator cannot disable the Bluetooth protocol stack, this is a finding. |
| 54 | The mobile operating system must detect if the security policy has been modified, disabled, or bypassed. | If the security policy has been modified in an unauthorized manner, security is severely degraded and a variety of further attacks are possible. Detecting whether the security policy has been modified or disabled mitigates these risks. | NIST SP 800-53, Rev3: CM-6 (1) | Review system documentation and security information resources to determine that the operating system has mechanisms to check the integrity of the code that enforces the security policy and that these controls have been effective in practice. Alternatively, the operating system or a third party mechanism can attempt to perform functions that should be prohibited. In this case, if these functions are permitted, this is evidence that the security policy has been modified or disabled. If the system does not have integrity verification or behavioral mechanisms to detect whether the security policy has been modified or disabled, this is a finding. |
| 55 | The mobile operating system must not permit a user to remove organizationally required applications. | Organizationally required applications are present on the device because they support the organization's mission. Therefore, their absence degrades mission performance. Preventing the removal of such applications provides mission assurance. | NIST SP 800-53, Rev3: CM-7 | Review system documentation and operating system configuration to determine if the operating system permits a user to remove organizationally required applications. Identify the list of organizationally required applications and attempt to delete a sample of them to determine if the control is being enforced. If a required application can be removed by a user, this is a finding. |
| 56 | The mobile operating system must verify the integrity of program software before permitting its execution. | A common method to compromise system security is to modify application software to perform malicious functions that will execute when the user runs the application. Verifying the integrity of the software before execution protects against such an attack. This is typically accomplished by checking cryptographic hashes or digital signatures on software program files. | NIST SP 800-53, Rev3: CM-7 (2) | Review system documentation and operating system configuration to determine if the operating system verifies the integrity of program software before permitting its execution. |
| 57 | The mobile operating system must employ automated mechanisms, per organization defined frequency, to detect the addition of unauthorized components/devices into the operating system. | If the user or an adversary is able to add unauthorized components to a device, then those components may be used to compromise other components or perform prohibited functions. The addition of the unauthorized component may also cause the system to behave in unintended ways, perhaps degrading the performance of mission-critical applications. Detecting the addition of unauthorized components allows for roll-back to the previous state. | NIST SP 800-53, Rev3: CM-8 (3) (a) | Inspect a sample of devices and develop a list of installed components on each of them. Compare this list against a list of authorized components. If the list of installed components contains items not on the list of authorized components, this is a finding. It is recommended that automated checks occur at least once every four hours if this is configurable. |
| 58 | The operating system must uniquely identify and must authenticate organizational users (or processes acting on behalf of organizational users). | To assure accountability and prevent unauthorized access, organizational users shall be identified and authenticated. | NIST SP 800-53, Rev3: IA-2 |  |
| 59 | The mobile operating system's Bluetooth module must support pairing using a randomly generated passkey size of at least 8 digits. | When done properly, Bluetooth pairing prevents rogue devices from communicating with the operating system. If a rogue device is paired with the mobile device, then there is the potential for the rogue device to obtain sensitive information. Short passkeys make the pairing process vulnerable to brute force attacks. The use of known fixed passkeys makes the device even more vulnerable. If device pairing is accomplished with a randomly generated 8-digit passkey, this greatly mitigates the risk of unauthorized pairing. | NIST SP 800-53, Rev3: IA-3 | Review the system documentation to determine if the Bluetooth stack supports passkeys of 8 digits or more. If greater assurance is required, attempt to pair the device with another Bluetooth device using an 8 digit passkey. If the Bluetooth stack does not support pairing using a randomly generated passkey size of at least 8 digits, this is a finding. |
| 60 | The mobile operating system's Bluetooth module must not permit any data transfer between devices prior to Bluetooth mutual authentication. | Bluetooth mutual authentication provides assurance that both the mobile device and Bluetooth peripheral are legitimate. If the authentication does not occur immediately before permitting a network connection, there is the potential for a man-in-the-middle attack in which a third device intercepts the traffic between the two legitimate devices. Mutual authentication prevents this from occurring. | NIST SP 800-53, Rev3: IA-3 | The local Bluetooth stack either supports this functionality or it does not. Review the system documentation to determine if the functionality is supported. If the Bluetooth stack permits any data transfer between devices prior to Bluetooth mutual authentication, this is a finding. |
| 61 | The mobile operating system's Wi-Fi module must be WPA2 certified (enterprise and personal). | WPA2 is a Wi-Fi certification managed by the Wi-Fi Alliance, a trade association promoting technology based on the IEEE 802.11 communications standard. A product that has received WPA2 certification has demonstrated that it is compliant with the 802.11i amendment defining robust security networks. Products that have not received this certification are significantly more likely to have vulnerabilities associated with user and device authentication and the confidentiality and integrity of user data. | NIST SP 800-53, Rev3: IA-3 (1) | Check the product documentation to verify the Wi-Fi interface of the mobile device is WPA2 certified. If it is not, this is a finding. |
| 62 | The mobile operating system must authenticate devices before establishing remote network (e.g., VPN) connections using bidirectional cryptographically based authentication between devices. | Without strong mutual authentication a mobile device may connect to an unauthorized network. In many cases, the user may falsely believe that the device is connected to an authorized network and then provide authentication credentials and other sensitive information. A strong bidirectional cryptographically based authentication method mitigates this risk. | NIST SP 800-53, Rev3: IA-3 (1) | Identify the network interfaces over which authentication may occur. For each of these, review the system documentation and operating system configuration to determine if the device authenticates devices prior to establishing a network connection. If the operating system does not perform this authentication, this is a finding. |
| 63 | The mobile operating system and MDM server must mutually authenticate each other using bi-directional PKI-based cryptographic authentication methods before transferring data. | Without strong mutual (bi-directional) authentication a mobile device may connect to an unauthorized MDM server and obtain improper security policies or configuration commands from that server. This could, in turn, make the device vulnerable to a wide variety of other attacks that could reveal sensitive information and enable an adversary to obtain full control of the device. Cryptographic mutual authentication greatly mitigates this risk. Shared secret methods are an acceptable alternative to PKI-based authentication. | NIST SP 800-53, Rev3: IA-3 (1) | Review system documentation and operating system configuration to determine if there is mutual authentication between the device and the MDM server. Both certificate-based and shared secret methods are acceptable. If there is not cryptographic mutual authentication, this is a finding. |
| 64 | The mobile operating system must verify all digital certificates in the certificate chain when performing PKI transactions. | If an adversary is able to compromise one of the certificates in the certificate chain, the adversary may be able to sign lower level certificates in the chain. This would enable the adversary to masquerade as other users or systems. By providing the mobile user with such false assurance, the adversary may be able obtain DOS information, capture authentication credentials, and perform other unauthorized functions. Verifying all digital certificates in the chain mitigates this risk. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation and operating system configuration to validate the operating system is verifying all digital certificates in the certificate chain when performing PKI transactions. If higher assurance is required, the reviewer should attempt to perform a transaction using a falsely signed certificate. If the certificate is accepted, the operating system is likely not performing the required check of root and intermediate certificates. If the DOS root and intermediate certificates are not present, this is a finding. |
| 65 | The mobile operating system must not accept certificate revocation information without verifying its authenticity. | If the operating system does not verify the authenticity of revocation information, there is the potential that an authorized system is providing false information. Acceptance of the false information could result in the installation of unauthorized software or connection to rogue networks, depending on the use for which the certificate is intended. Verifying the authenticity of revocation information mitigates this risk. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Inspect readily available configuration settings if these are available. Otherwise, if feasible, test the system with a known revoked certificate and revocation status information signed by an unauthorized entity. The system should be able to detect that the revocation status information is not authentic. If the system does not verify the authenticity of revocation information, this is a finding. |
| 66 | The mobile operating system must give the user the option to deny acceptance of a certificate if the mobile operating system determines that the certificate is invalid. | When the operating system accepts the use of invalid certificates, there is the potential that the system presenting the certificate is malicious, and can compromise sensitive information or system integrity. Allowing the operating system or user to deny invalid certificates mitigates the risk associated with the acceptance of such certificates. | NIST SP 800-53, Rev3: IA-5 (2) | Review the operating system configuration and system documentation to determine how to enable a user to prevent communication with other systems when they present an invalid certificate. Verify the correct settings have been selected. Alternatively, visit a website with a known invalid certificate and test whether the user is provided the option to reject the certificate. If the operating system does not allow the user to reject the certificate when it is invalid, this is a finding. |
| 67 | The mobile operating system must alert the user if it receives an invalid public-key certificate. | If the user is aware that a certificate is invalid, the user can opt not to proceed or, alternatively, is better prepared to identify suspicious behavior that indicates a security incident is in progress. Failure to notify the user of this occurrence makes it more likely that an adversary can launch an attack from an untrusted system. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Check that the operating system has the capability to alert the user when it has received an invalid public-key certificate. Otherwise, direct the operating system to a resource with a known invalid certificate to verify it correctly notifies the user of the invalid state of the certificate. If the system does not alert the user when it receives an invalid public-key certificate, this is a finding. |
| 68 | The mobile operating system must give the user the option to deny acceptance of a certificate if the certificate was issued by an untrusted certificate authority. | When the operating system accepts the use of certificates issued from an untrusted certificate authority, there is the potential that the system presenting the certificate is malicious, and can compromise sensitive information or system integrity. Allowing the operating system or user to deny certificates from an untrusted certificate authority mitigates the risk associated with the acceptance of such certificates. | NIST SP 800-53, Rev3: IA-5 (2) | Review the operating system configuration and system documentation to determine how to enable a user to prevent communication with other systems when they present a certificate issued by an untrusted certificate authority. Verify the correct settings have been selected. Alternatively, visit a website with a known untrusted certificate and test whether the user is provided the option to reject the certificate. If the operating system does not allow the user to reject the certificate when it is from an untrusted certificate authority, this is a finding. |
| 69 | The mobile operating system must alert the user if it receives a public-key certificate issued from an untrusted certificate authority. | If the user is aware that a certificate has been issued from an untrusted certificate authority, the user can opt not to proceed or, alternatively, is better prepared to identify suspicious behavior that indicates a security incident is in progress. Failure to notify the user of this occurrence makes it more likely that an adversary can launch an attack from an untrusted system. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Check that the operating system has the capability to alert the user when it has received a public-key certificate issued from an untrusted certificate authority. Otherwise, direct the operating system to a resource with a known untrusted certificate to verify it correctly notifies the user of the untrusted state of the certificate. If the operating system does not alert the user when it receives a certificate from an untrusted certificate authority, this is a finding. |
| 70 | The mobile operating system must give the user the option to deny acceptance of a certificate if it cannot verify the certificate's revocation status. | When additional assurance is required, the system should deny acceptance of a certificate if it cannot verify its revocation status. Otherwise, there is the potential that it is accepting the credentials of an unauthorized system. Allowing the operating system or user to deny certificates with unverified revocation status mitigates the risk associated with the acceptance of such certificates. | NIST SP 800-53, Rev3: IA-5 (2) | Review the operating system configuration and system documentation to determine how to enable a user to prevent communication with other systems when they present a revoked certificate. Verify the correct settings have been selected. If the operating system does not allow the user to reject the certificate when it cannot validate the certificate's revocation status, this is a finding. |
| 71 | The mobile operating system must query the certification authority to determine whether a public-key certificate has been revoked before accepting the certificate for authentication purposes. | Failure to verify a certificate's revocation status can result in the system accepting a revoked and therefore authorized certificate. This could result in the installation of unauthorized software or connection for rogue networks, depending on the use for which the certificate is intended. Querying for certificate revocation mitigates the risk that the system will accept an unauthorized certificate. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Inspect readily available configuration settings if these are available. Otherwise, test the system with a known revoked certificate to determine whether the operating system properly rejects further transactions with the system or object presenting the revoked certificate. If the system accepts a revoked certificate or is configured not to check for certificate revocation, this is a finding. |
| 72 | The mobile operating system must notify the user if it cannot verify the revocation status of the certificate. | If the user is aware that the revocation status of a certificate could not be verified, the user is better prepared to identify suspicious behavior that indicates a security incident is in progress. Failure to notify the user of this occurrence makes it more likely that an adversary can use revoked certificates without detection. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Inspect readily available configuration settings if these are available. Check that the capability to notify the user when the operating system cannot verify a certificate's revocation status is enabled. Otherwise, disable the ability of the operating system to access information on the revocation status of the certificate and then test the system with a known good certificate. To disable access on verification status, the device can be placed on a segregated network for the test. If the system does not notify the user that it was unable to verify the revocation status of the certificate, this is a finding. |
| 73 | The mobile operating system must require a password to access private keys saved in the key certificate store. | The cornerstone of the PKI is the private key used to encrypt or digitally sign information. Allowing unauthenticated access to private keys can enable an adversary in possession of the device to decrypt messages encrypted with the public key and to digitally sign data, thereby potentially enabling an adversary to impersonate the user in any application that uses that private key for user authentication. Requiring a password to access keys saved in the certificate store mitigates the risk of unauthorized access. | NIST SP 800-53, Rev3: IA-5 (2) | Attempt to perform a transaction that requires access to the private key. If the operating system does not prompt the user for a password, this is a finding. |
| 74 | The mobile operating system must enforce the same complexity requirements for the password needed to access private keys at is does for the device unlock password. | The cornerstone of the PKI is the private key used to encrypt or digitally sign information. A weak password may enable an adversary to crack it, and give it the ability to use the private key to decrypt sensitive information or improperly impersonate the user of the device. | NIST SP 800-53, Rev3: IA-5 (2) | Review system documentation to determine the expected behavior of the system. Inspect the available password complexity configuration to determine if it meets requirements. If this is not feasible, attempt to set a non-compliant password on the key and verify the operating system rejects it. Note: It is permissible for the operating system to use a single password for both devices unlock and access to private keys. If the system does not require a password, or does not enforce the complexity requirements, this is a finding. |
| 75 | The mobile operating system browser must support public-key certificate-based authentication to remote information systems. | The cornerstone of the PKI is the private key used to encrypt or digitally sign information. The key by itself is a cryptographic value that does not contain specific user information. The authenticated identity must be mapped to an account for access and authorization decisions. This capability strengthens authentication to remote information systems and thus makes it less likely that such systems will be compromised. | NIST SP 800-53, Rev3: IA-5 (2) | Direct the browser to a DOS web site requiring certificate-based authentication. Verify a user can authenticate to such a site. If it is apparent that a user cannot authenticate to a DOS-web site because of the absence of certificate authentication support, this is a finding. |
| 76 | The mobile operating system must encrypt passwords stored on the mobile device. | Passwords need to be protected at all times and encryption is the standard method for protecting passwords while in storage so unauthorized users/processes cannot gain access. If an adversary obtains a password, the adversary can use it to compromise sensitive information. Encrypting passwords stored on the device mitigates the risk that the passwords will be compromised. | NIST SP 800-53, Rev3: IA-5 (1) (c) | Super user access is typically required to access the password database. If a system administrator is able to obtain this level of privilege on the device, have the system administrator display the contents of the password database, often a simple file. Verify the passwords contained in the database are encrypted. If it is not possible to view the password database, review system documentation and security information resources to determine if the operating system encrypts passwords. If it is apparent that the passwords stored on the device are not encrypted, this is a finding. |
| 77 | The mobile operating system must not transmit passwords in clear text. | Transmission of passwords in clear text reveals the password to any adversary who can successfully eavesdrop on the communication. In the case of wireless communication, the ability to eavesdrop is available to anyone within the range of the device's radio signal, which in some cases can be miles. Once an adversary has obtained a password, the adversary may be able to use it to compromise sensitive DOS information or other DOS information systems. Using methods that avoid the transmission of passwords in clear text mitigates the risk of this attack. | NIST SP 800-53, Rev3: IA-5 (1) (c) | Review system documentation and security information resources to determine if it is possible to transmit passwords in clear text. If doubt remains and resources permit, the device may be tested using a network protocol analyzer to determine if an entered password is transmitted in clear text. If it is determined that the system transmits passwords in clear text, this is a finding. |
| 78 | The mobile operating system must enforce a maximum lifetime of 60 days for the device unlock password (password age). | The ability to crack a password is a function of how many times can attempt to crack the password, how quickly the adversary can do each attempt, and the size of the password space. Any password no matter how complex can eventually be cracked. Periodically changing the password makes it less likely that the password will be cracked because the adversary cannot eliminate previously known incorrect passwords when entering additional attempts. | NIST SP 800-53, Rev3: IA-5 (1) (d) | Review the operating system configuration settings to determine if there is a compliant maximum password age setting. If the operating system cannot enforce password aging, this is a finding. |
|  |  |  |  |  |
|  |  |  | DOS 12 FAM 622.1-3 (J) (1) |  |
| 79 | The mobile operating system must prohibit a user from reusing any of the last 24 previously used device unlock passwords. | Password complexity, or strength, is a measure of the effectiveness of a password in resisting guessing and brute force attacks. Remembering the prior five device unlock passwords enables the operating system from permitting those passwords to be reused, which increases the resistance against password attacks. | NIST SP 800-53, Rev3: IA-5 (1) | Review the operating system configuration settings to determine if there is prohibition against reusing a previously used device unlock password. If the setting is not configurable and compliance cannot be determined from system documentation, have a user change their password twice, the second time to the original password. If the operating system enforces a password history of greater than the previous five passwords, this is acceptable. If the operating system allows the reversion to the original password, this is a finding. |
|  |  |  |  |  |
|  |  |  |  |  |
| 80 | The mobile operating system must enforce a minimum length of 12 characters for the device unlock password. | Password complexity, or strength, is a measure of the effectiveness of a password in resisting guessing and brute force attacks. The ability to crack a password is a function of how many times an attempt to crack the password, how quickly the adversary can do each attempt, and the size of the password space. The longer the minimum length of the password is, the larger the password space. | NIST SP 800-53, Rev3: IA-5 (1) (a) | Review system documentation and the operating system configuration to determine if the device enforces a minimum length for the device unlock password. If the device does not enforce a minimum length for the device unlock password, this is a finding. |
|  |
| DOS 12 FAM 622.1-3 (J) (3) |
| 81 | The mobile operating system must obscure passwords on the device's display when they are entered on the device. | To prevent the compromise of authentication information, such as passwords during the authentication process, the feedback from the operating system shall not provide any information allowing an unauthorized user to compromise the authentication mechanism. Otherwise, someone nearby the user (a.k.a., "shoulder surfer") may be able to obtain the password through visual observation. | NIST SP 800-53, Rev3: IA-6 | Attempt to enter a password on the device and note whether the characters are obscured with asterisks or by other means. It is acceptable for the passwords to be revealed for very brief periods of time (less than a second) so the user can verify if the character was entered correctly. If the operating system does not otherwise hide passwords as they are entered, this is a finding. |
| 82 | The mobile operating system must cryptographically bind the removable media to the mobile device so data stored on the media card can only be read by that mobile device. | When data is written to portable digital media, such as thumb drives, floppy diskettes, compact disks, and magnetic tape, etc., there is risk of data loss. Cryptographically binding the removable media to the mobile device renders the media useless when it is separated from the device. This greatly reduces the risk associated with removable media. | NIST SP 800-53, Rev3: MP-2 (2) | On a sample of devices, remove the portable media (e.g., SD card) from the device and attempt to read its contents from another device. If the contents are readable, this is a finding. Review the system documentation and operating system configuration to determine if the binding capability is present. If there no evidence the system provides this capability, this is a finding. |
| 83 | The mobile operating system must use automated mechanisms to detect the presence of unauthorized software on organizational information systems and notify designated organizational officials in accordance with the organization defined frequency. | Authorized software poses a risk to the device because it could potentially perform malicious functions, including but not limited to gathering sensitive information, searching for other system vulnerabilities, or modifying log entries. A mechanism to detect unauthorized software and notify officials of its presence assists in the task of removing such software to eliminate the risks it poses to the device and the networks to which the device attaches. | NIST SP 800-53, Rev3: CM-8 | Review system documentation and operating system configuration to determine whether and how the operating system detects and reports the presence of unauthorized software. If feasible, install a test application that is authorized for such purpose, but which the system does not recognize as authorized. Verify the operating system detects the test application and reports it. If the operating system either fails to detect an authorized application or fails to report this (or both), this is a finding. |
| 84 | The mobile operating system must prevent a user from installing unapproved applications. | The operating system must enforce software installation by users based upon what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect) by the organization. The installation and execution of unauthorized software on an operating system may allow the application to obtain sensitive information or further compromise the system. Preventing a user from installing unapproved applications mitigates this risk. | NIST SP 800-53, Rev3: CM-11 , SI-7 | Review system documentation and operating system configuration to determine if there are controls that prevent a user from installing unapproved applications. Typical ways this might be accomplished is through enforcement of application "white lists", requiring super user privileges to install applications, and forcing the device to only install applications from designated application repositories that are controlled by a system administrator. If none of these controls are present, this is a finding. |
| 85 | The mobile operating system must only permit download of software from a DOS approved source (e.g., DOS operated mobile device application store or MDM server). | DOS can perform due diligence on sources of software to mitigate the risk that malicious software is introduced to those sources. Therefore, if software is downloaded from a DOS approved source, then it is less likely to be malicious than if it is downloaded from an unapproved source. To prevent access to unapproved sources, the operating system in most cases can be configured to disable user access to public application stores. | NIST SP 800-53, Rev3: CM-11 , SI-7 | Examine the operating system configuration and documentation to determine how it obtains application and other software. Validate it has a mechanism to limit download to one or more sources. Then verify the directed sources are DOS approved. If the operating system has no mechanism to limit the source of software, this is a finding. If the operating system is configured to restrict the source of software, but still allows download from an unapproved site, this is a finding. |
| 86 | Users must not be allowed to download applications on mobile operating system devices without system administrator control (i.e., the SA either downloads and installs the application or enables the user to download/install the application). | The installation and execution of unauthorized software on an operating system may allow the application to obtain sensitive information or further compromise the system. If the system administrator has control over what applications are downloaded, then the system administrator can check that only known good programs are installed, which significantly mitigates the risk posed by malicious software. | NIST SP 800-53, Rev3: CM-11 , SI-7 | Review system documentation and operating system configuration to determine if the system administrator has the ability to prevent a user from downloading an application outside of the system administrator's control. Typical ways this might be accomplished is through enforcement of application "white lists", requiring super user privileges to install applications, and forcing the device to only install applications from designated application repositories that are controlled by a system administrator. If none of these controls are present, this is a finding. |
| 87 | The mobile operating system must terminate the network connection associated with a communications session at the end of the session or after an organization defined time period of inactivity. | If communications sessions remain open for extended periods of time even when unused, there is the potential for an adversary to highjack the session and use it to gain access to the device or networks to which it is attached. Terminating sessions after a certain period of inactivity is a method for mitigating the risk of this vulnerability. | NIST SP 800-53, Rev3: SC-10 | Review system documentation and operating system configuration to verify the operating system terminates network connections after an organization defined time period of inactivity. If greater assurance of compliance is desired, wait for the organizationally defined period on a sample device to verify the system terminates the session when it is inactive. If communications are not terminated after an organization defined time period of inactivity, this is a finding. |
| 88 | The mobile operating system must establish a trusted communications path for the user to enter the device unlock password (e.g., to prevent key logging). | A common operating system attack is to install a key logger or other software that can capture a user's authentication credentials when the user enters them. A trusted communications path is one in which there is a high degree of assurance that there are no intermediaries between the input and the security enforcement code that handles the authentication transaction. Establishing a trusted communications path for the entry of the device unlock password greatly reduces the risk that the password will be compromised. | NIST SP 800-53, Rev3: SC-11 | Review system documentation and security information resources to determine if the operating system establishes a trusted path for the user to enter the device unlock password. If the operating system does not provide a trusted path, this is a finding. |
| 89 | The mobile device operating system must have access to DOS root and intermediate PKI certificates when performing DOS PKI related transactions. | DOS root and intermediate PKI certificates are used to verify the authenticity of PKI certificates of users and web services. If the root and intermediate certificates are not available, an adversary could falsely sign a certificate in such a way that it could not be detected. Providing access to the DOS root and intermediate PKI certificates greatly diminishes the risk of this attack. | NIST SP 800-53, Rev3: SC-12 | On a sample of devices, review the operating system configuration to determine if the root and intermediate certificates are present. In some cases, their presence may not be detected by user inspection, in which case the reviewer should review system documentation to determine whether they are present. If higher assurance is required, the reviewer should attempt to perform a transaction using a falsely signed certificate. If the certificate is accepted, the operating system is likely not performing the required check of root and intermediate certificates. If the DOS root and intermediate certificates are not present, this is a finding. |
| 90 | The mobile operating system PKI certificate store must encrypt contents using AES encryption (AES 128 bit encryption key length is the minimum requirement; AES 256 desired). | If an adversary can access the key store, it may be able to use the keys to perform a variety of unauthorized transactions. It may also be able to modify public keys in a way that it can trick the operating system into accepting invalid certificates. Encrypting the key store protects the integrity and confidentiality of keys. AES encryption with adequate key lengths provides assurance that the protection is strong. | NIST SP 800-53, Rev3: SC-12 | Review system documentation and operating system configuration to determine if the operating system uses AES encryption with 128-bit or longer keys to encrypt the contents of the key store. If the key store is not encrypted or does not use AES encryption, this is a finding. |
| 91 | The mobile operating system must support both software-based and hardware-based public-key certificates (Smart Card / PIV). | Software-based certificates are required to authenticate many web sites. Hardware-based certificate support is needed to support the DOS Smart Card. Without both software and hardware-based certificate support, there is the potential that critical authentication transactions cannot occur. This will either hinder performance of the mission or degrade the security posture of one or more applications. If the operating system can support both software and hardware-based certificates, this provides assurance that all required certificate-based transactions are supported. | NIST SP 800-53, Rev3: SC-12 | Review system documentation and operating system configuration to verify both software-based and hardware-based certificates are supported. Attempt to access a web site that requires a software-based certificate to verify the operating system supports software-based certificates. Attempt to send a digitally signed DOS email to verify the operating system supports hardware-based certificates. If the operating system fails to support either software-based or hardware-based certificates, this is a finding. |
| 92 | The cryptographic module supporting encryption of data at rest must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 93 | The cryptographic module supporting the VPN client security functions must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 94 | The mobile operating system PKI certificate store must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 95 | The cryptographic module supporting encryption of the certificate store must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 96 | The mobile operating system must alert the user or system if a non-FIPS approved algorithm is specified in a PKI certificate. | FIPS approved cryptographic algorithms have been thoroughly reviewed for their strength against cryptographic attacks. Non-FIPS algorithms are significantly more likely to be vulnerable. If the operating system does not alert when a transaction involves a non-FIPS approved algorithm, there is the potential that an adversary can trick the system into using weak cryptography that the adversary can crack. Providing an alert enables the user or system to abort the transaction and thereby eliminate the risk. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation and operating system configuration to determine if the system provides an alert if a non-FIPS algorithm is used in a certificate. If greater assurance is required, attempt to perform a transaction with a certificate that uses a non-FIPS approved algorithm and verify the operating system sends an alert. If the module does not alert in this case, this is a finding. |
| 97 | The cryptographic module supporting Bluetooth data communications must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 98 | The cryptographic module supporting Wi-Fi security functions must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 99 | The cryptographic module supporting encryption of data in transit (including email and attachments) must be FIPS 140-2 validated. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. | NIST SP 800-53, Rev3: SC-13 (1) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. |
| 100 | The operating system must employ FIPS validated cryptography to protect information when it must be separated from individuals who have the necessary clearances, yet lack the necessary access approvals. | Cryptography is only as strong as the encryption modules/algorithms employed to encrypt the data. | NIST SP 800-53, Rev3: SC-13 (3) | Verify the operating system employs FIPS validated cryptography. If the operating system does not employ FIPS validated cryptography, this is a finding. |
| 101 | The mobile operating system must employ FIPS validated or NSA approved cryptography to implement digital signatures. | The most common vulnerabilities with cryptographic modules are those associated with poor implementation. FIPS 140 validation and NSA approval provides assurance that the relevant cryptography has been implemented correctly. FIPS validation is also a strict requirement for use of cryptography in the Federal Government. Similarly, NSA approval of cryptography for classified data and applications is a strict requirement. | NIST SP 800-53, Rev3: SC-13 (4) | Review system documentation to identify the FIPS 140 certificate for the cryptographic module. Visit the NIST web site http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm to verify the certificate is still valid. If the module is not currently FIPS validated, this is a finding. Similarly, if NSA approved cryptography is not used to implement digital signatures for classified systems, this is a finding. |
| 102 | The mobile operating system must prohibit remote activation of collaborative computing functions, including microphones, cameras, and networked white boards without user concurrence. | If an adversary can remotely activate collaborative computing functions, the adversary may be able to listen to the user's conversations, obtain visual data about the user's surroundings, or read sensitive information on the display of the user's device. To mitigate these risks, only a user in immediate possession of the device should be able to activate these functions. | NIST SP 800-53, Rev3: SC-15 a | Review system documentation and both operating system and application configuration to determine if it is possible to remotely activate collaborative computing functions. Also, review security information resources to determine if such vulnerabilities have been reported on devices running this operating system. If it is possible to remotely activate a collaborative computing function, this is a finding. |
| 103 | The mobile operating system must block both inbound and outbound instant message (IM) traffic for all non-DOS authorized IM systems. | Many instant messaging systems have known vulnerabilities, some of which allow an adversary to install malware on the device. This malware can then be used to obtain sensitive information or further compromise DOS information systems. Restricting IM traffic to DOS authorized IM systems mitigates the risk of using IM technology. | NIST SP 800-53, Rev3: SC-15 (2) | Inspect a sample of devices to determine if there are any non-authorized IM applications on the device. If there are, ensure these systems cannot be used for either inbound or outbound traffic by attempting to transmit a message from the device and possibly sending a message to the device. If the system can perform any messaging function on an unauthorized IM application, this is a finding. |
| 104 | The mobile operating system must grant a downloaded application only those permissions specified in the application's manifest. | Mobile operating system applications that are able to perform unintended functions may be able to obtain sensitive information or otherwise compromise system security. The permissions that an application requires to perform its function are typically delineated in a manifest that is bound to the application and granted during the installation process. Enforcing these permissions limitations is necessary to ensure the application is not permitted to perform unintended functions. | NIST SP 800-53, Rev3: SC-16 | Review security information resources to determine if the operating system enforces manifest privileges as advertised. Use a tool (e.g., Fixmo Sentinel) that checks to determine if an application is permitted to perform restricted functions. If it is determined that manifest permissions are not enforced, this is a finding. |
| 105 | The mobile operating system must validate the integrity of a downloaded application's manifest before granting the application permissions on the device. | If an adversary can modify an application's manifest, then the adversary can add additional permissions that would enable it to perform unauthorized functions. These functions could enable the adversary to obtain sensitive information or compromise other aspects of system security. Validating the integrity of the manifest mitigates the risk that an adversary has modified its contents. | NIST SP 800-53, Rev3: SC-16 (1) | Review system documentation, operating system configuration, and other security information resources to determine if the operating system validates the integrity of each downloaded application's manifest. If it is determined that the integrity check is not occurring, this is a finding. |
| 106 | Only DOS PKI issued or approved software authentication certificates must be installed on DOS mobile operating system devices. | If unauthorized software authentication certificates are installed on the device, then the operating system would not block malware signed by the entity that published these certificates. Such malware could be used to obtain sensitive DOS information or to further breach system security. Eliminating unapproved software authentication certificates greatly mitigates the risk of malware passing authentication controls. | NIST SP 800-53, Rev3: SC-17 | On a sample of devices, check the certificate store that contains the software authentication certificates. In some cases, the certificates may not be visible. In this situation, consult system documentation to determine what certificates are installed on the device. Match the certificates present against a list of approved certificates. Verify there are no unapproved certificates present. If there is unapproved software authentication certificates installed on the device, this is a finding. |
| 107 | Only DOS PKI issued or approved device authentication certificates must be installed on DOS mobile operating system devices. | If unauthorized device authentication certificates are installed on the device, there is the potential that the device may connect to a rogue device or network. Rogue devices can mimic the behavior of authorized equipment to trick the user into providing authentication credentials, which could then in turn be used to compromise DOS information and networks. Restricting device authentication certificates to an authorized list mitigates the risk of attaching to rogue devices and networks. | NIST SP 800-53, Rev3: SC-17 | On a sample of devices, check the certificate store that contains the device authentication certificates. In some cases, the certificates may not be visible. In this situation, consult system documentation to determine what certificates are installed on the device. Match the certificates present against a list of approved certificates. Verify there are no unapproved certificates present. If there is unapproved device authentication certificates installed on the device, this is a finding. |
| 108 | The operating system must prevent the download of prohibited mobile code. | Decisions regarding the employment of mobile code within operating systems are based on the potential for the code to cause damage to the system if used maliciously. | NIST SP 800-53, Rev3: SC-18 (3) | Attempt to download prohibited mobile code to see if the operating system prohibits the action. If download is successful, this is a finding. |
| 109 | The mobile operating system must require a valid password be successfully entered before the mobile device data is unencrypted. | Encryption is only effective if the decryption procedure is protected. If an adversary can easily access the private key (either directly or through a software application), then sensitive DOS data is likely to be disclosed. Password protection is one method to reduce the likelihood of such an occurrence. | NIST SP 800-53, Rev3: SC-28 (1) | On a sample of devices known to encrypt information resident on the devices, attempt to access an encrypted file and verify the operating system prompts for a password. If data is accessible without entering a password at some point when using the device, this is a finding. |
| 110 | The mobile operating system must re-encrypt all device data when the device is locked. | If data is not encrypted upon the lock of the device, there is the potential for an adversary to remove non-volatile memory from the device and read it directly using tools for that purpose. This attack would render other operating system controls useless. Encrypting data provides assurance that it will be protected even when memory is physically removed from the device. | NIST SP 800-53, Rev3: SC-28 (1) | Review system documentation and other security information resources to determine how the operating system treats data in memory upon the lock of the device. The operating system may enforce this requirement in a variety of means. The reviewer should focus on the fact that the data is encrypted when the device has been shut down suddenly and not on the timing of the encryption, much of which might occur prior to device lock. If it is determined that unencrypted data still resides on the device after device lock, this is a finding. |
| 111 | The mobile operating system must encrypt all data on the mobile device using AES encryption (AES 128 bit encryption key length is the minimum requirement; AES 256 desired). | If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running. AES encryption with appropriate key lengths provides assurance that the cryptography is adequate. | NIST SP 800-53, Rev3: SC-28 (1) | Review system documentation and operating system configuration to verify the operating system encrypts all data using AES encryption. Validate this includes data on removable memory, such as SD cards. If the operating system does not encrypt data at rest, or does so only selectively, or does so using an encryption algorithm other than AES (for unclassified data), this is a finding. |
| 112 | The mobile operating system must prevent DOS applications from accessing non-DOS data when the device supports multiple user environments (e.g., work and personal) if such access has not been approved. | In many cases, the presence of non-DOS data on DOS information systems violates either local or department guidelines. When a device is used for more than one purpose (e.g., work and personal) there is the potential for information from one environment to migrate inappropriately over into another environment. The operating system must prevent this occurrence using appropriate technical controls that mitigate the risk of data leakage. The objective is to provide appropriate separation between each environment on the device. | NIST SP 800-53, Rev3: SC-4 | Review system documentation and operating system configuration to determine if the device supports multiple user environments. If it does, verify the operating system has control for preventing DOS applications from accessing non-DOS data. On a sample of devices, attempt to access non-DOS data from a DOS application. If non-DOS data can be accessed from a DOS application, this is a finding. |
| 113 | The mobile operating system must prevent non-DOS applications from accessing DOS data when the device supports multiple user environments (e.g., work and personal). | When a device is used for more than one purpose (e.g., work and personal) there is the potential for information from one environment to migrate inappropriately over into another environment. The operating system must prevent this occurrence using appropriate technical controls that mitigate the risk of data leakage. The objective is to provide appropriate separation between each environment on the device. | NIST SP 800-53, Rev3: SC-4 | Review system documentation and operating system configuration to determine if the device supports multiple user environments. If it does, verify the operating system has control for preventing non-DOS applications from accessing DOS data. On a sample of devices, attempt to access DOS data from a non-DOS application. The most straightforward way to accomplish this is to determine if DOS storage partitions are available to non-DOS applications when storing or reading a file on the DOS partition. If non-DOS applications can access DOS data, this is a finding. |
| 114 | The mobile operating system's Bluetooth module must support the capability for a system administrator to create a non-user-modifiable white list of Bluetooth devices that are authorized to pair to the mobile device. | If a rogue device can connect to the mobile device, there is the potential for the rogue device to obtain sensitive information. One mechanism for preventing this occurrence is to enforce a "white list" of devices that are permitted to pair to the mobile device. Devices not on the white list will not be able to pair with the mobile device and therefore cannot communicate with it or obtain sensitive information from it. | NIST SP 800-53, Rev3: SC-7 (5) | Examine the operating system configuration to verify the presence of a white list of Bluetooth devices authorized to pair to the mobile device. If the operating system does not support this functionality, this is a finding. If the operating system supports the white list functionality, attempt to pair a test Bluetooth device not on the white list with the mobile device. If it successfully pairs, this is a finding. |
| 115 | The mobile operating system VPN client must disable split tunneling. | When split-tunneling is enabled, device peripherals and other computers communicating with the mobile device may be able to connect a DOS network and obtain sensitive information or otherwise compromise DOS information resources. Disabling split tunneling eliminates the risk associated with this vulnerability. | NIST SP 800-53, Rev3: SC-7 (7) | Review the system documentation and operating system configuration to determine if split tunneling is disabled. If split tunneling is not disabled, this is a finding. |
| 116 | The mobile operating system must be able to filter both inbound and outbound traffic based on IP address and UDP/TCP port. (As controlled by MDM) | Open ports provide an attack surface that an adversary can then potentially use to breach system security. If an adversary can communicate with the mobile device from any IP address, then the device may be open to any other device on the Internet. Reducing the attack surface through IP address and port restrictions mitigates this risk. | NIST SP 800-53, Rev3: SC-7 (12) | Review the system documentation and operating system configuration to determine if the operating system is able to filter both inbound and outbound traffic based on IP address and TCP/UDP port. If the operating system cannot support this functionality, this is a finding. |
| 117 | The mobile operating system must encrypt all data in transit using AES encryption when communicating with DOS information resources (128-bit key length is the minimum requirement; 256-bit desired). | If data traffic is sent unencrypted, an adversary may be able to read it to obtain sensitive information. AES encryption with 128-bit (or longer) keys mitigates the risk of unauthorized eavesdropping. This requirement applies to both VPN connections and DOS messaging connections (email and authorized instant messaging applications). | NIST SP 800-53, Rev3: SC-8 | Review the operating system documentation and configuration (and possibly application configuration) to determine if the system uses AES encryption with at least 128-bit keys. If it does not use AES encryption with the required key length, this is a finding. |
| 118 | The mobile operating system's VPN client must use either IPSec or SSL/TLS when connecting to DOS networks. | Use of non-standard communications protocols can affect both the availability and confidentiality of communications. IPSec and SSL/TLS are both well-known and tested protocols that provide strong assurance with respect to both security and interoperability. | NIST SP 800-53, Rev3: SC-8 | Review system documentation and operating system configuration to verify the VPN client uses IPSec or SSL/TLS when connecting to DOS networks. If it does not support either of these protocols, or does not use them when establishing a VPN connection to a DOS network, this is a finding. |
| 119 | The mobile operating system's Bluetooth stack must use 128-bit Bluetooth encryption when communicating with other Bluetooth devices. | If data traffic is sent unencrypted, an adversary may be able to read it to obtain sensitive information. 128-bit Bluetooth encryption mitigates the risk of unauthorized eavesdropping. | NIST SP 800-53, Rev3: SC-8 | Review system documentation and operating system configuration to verify the device's Bluetooth stack supports 128-bit Bluetooth encryption and uses it for all data connections. If the Bluetooth module does not support 128-bit Bluetooth encryption or does not use it when connecting with other devices, this is a finding. |
| 120 | The mobile operating system must detect and report the version of the operating system, device drivers, and application software when queried by an authorized entity. | Organizations are required to identify information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and report this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). To support this requirement, an automated process or mechanism is required. | NIST SP 800-53, Rev3: SI-2 (2) | On a sample of devices, use the MDM or another network management tool to query the device. Determine if it can identify the version of the operating system, selected device drivers, and at least one software application. If any such information cannot be obtained, this is a finding. |
| 121 | The mobile operating system must support automated patch management tools to facilitate flaw remediation of all software components on the device. | The organization (including any contractor to the organization) must promptly install security relevant software updates (e.g., patches, service packs, hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, must also be addressed. Left un-patched, software may be vulnerable to a variety of exploits that could disclose sensitive information or lead to subsequent security breaches. An automated patch management tool can mitigate this risk. | NIST SP 800-53, Rev3: SI-2 | Verify the presence of the automated patch management tool. Review the audit logs of the operating system or patch management tool to verify patches are occurring as expected. Also use version querying tools to validate the information in the logs. If there is no patch management system or it is not functioning as expected, this is a finding. |
| 122 | The mobile operating system must employ a DOS approved anti-virus application or otherwise prevent a malware application from installing and executing. | In order to minimize potential negative impact to the organization that can be caused by malicious code, it is imperative that malicious code is identified and eradicated. Malicious code includes viruses, worms, Trojan horses, and spyware. Malicious code can result in the disclosure of sensitive information or cause a denial of service. Anti-virus applications are not common on mobile operating systems but one or more methods to mitigate the risk of malware must be in place to protect DOS information and networks. | NIST SP 800-53, Rev3: SI-3 a | Review system documentation to determine the approach to malware prevention. This may include secure operating system architectures, mandatory access controls, and high-assurance authentication of code. Inspect the operating system to validate the approach has been implemented as claimed. If the approach has not been implemented, or if the implementation is inadequate, this is a finding. |
| 123 | The mobile operating system must prevent non-privileged users from circumventing malicious code protection capabilities. | A common tactic of malware is to identify the type of malicious code protection software running on the system and deactivate it, which enables subsequent attacks. If malicious code protection is itself protected, then it will prevent a non-privileged user or malicious software from disabling the protection mechanism. | NIST SP 800-53, Rev3: SI-3 (3) | Review the system documentation to determine if the malicious code protection capabilities are adequate. In particular, the protection mechanisms must load during the boot process and must not be able to be disabled. Reboot a device and verify the protection mechanisms are active after the boot cycle. Attempt to kill the protection process if it is identifiable. If the reviewer can disable the malicious code protection capabilities, this is a finding. |
| 124 | The mobile operating system must prevent non-privileged users from circumventing intrusion detection and prevention capabilities. | Intrusion detection and prevention capabilities must be architected and implemented to prevent non-privileged users from circumventing such protections. This can be accomplished through the use of user roles, use of proper systems permissions, auditing, logging, etc. | NIST SP 800-53, Rev3: AC-6 | Review system documentation, operating system configuration, and other security information resources to determine if a non-privileged user can circumvent intrusion detection and prevention capabilities. Determine if a non-privileged user can terminate processes for the intrusion detection and prevention functionality. If a non-privileged user can circumvent this functionality, this is a finding. |
| 125 | The mobile operating system must prevent a user from using a browser that does not direct its traffic to a DOS proxy server. | Proxy servers can inspect traffic for malware and other signs of a security attack. Allowing a mobile device to access the public Internet without proxy server inspection forgoes the protection that the proxy server would otherwise provide. Malware downloaded onto the device could have a wide variety of malicious consequences, including loss of sensitive DOS information. Forcing traffic to flow through a proxy server greatly mitigates the risk of access to public Internet resources. | NIST SP 800-53, Rev3: AC-6 | Review the operating system and browser configuration to determine if traffic is forced through DOS proxy servers. If greater assurance is required, access a number of Internet web sites and verify traffic flows through a DOS proxy server by viewing the traffic using a network protocol analyzer or by communicating with personnel that manage the proxy server. If the device accesses any internet resource without being directed through a DOS proxy server, this is a finding. |
| 126 | The mobile operating system must protect information obtained from intrusion and integrity monitoring tools from unauthorized access, modification, and deletion. | If an adversary can modify or delete information obtained from intrusion and integrity tools, then the adversary can hide evidence of an attack. Mechanisms to protect such data are necessary to mitigate the risk of these attacks and ensure they are detected in a timely manner. | NIST SP 800-53, Rev3: SI-4 | Review system documentation and operating system configuration to verify data collected by intrusion and integrity monitoring tools is either encrypted or sufficiently protected with file permissions not available to processes running user applications. If the reviewer has obtained evidence that modification or deletion of such data is possible, or if the reviewer can modify such data directly, this is a finding. |
| 127 | The mobile operating system must alert the MDM or Intrusion Detection and Prevention System (IDPS) when it has detected integrity check failures. | Successful incident response and auditing relies on timely, accurate system information and analysis in order to allow the organization to identify and respond to potential incidents in a proficient manner. Alerting an MDM or IDPS mitigates the potential for attacks triggering integrity failures to have further consequences to the enterprise. | NIST SP 800-53, Rev3: SI-4 (12) | Review system documentation and operating system configuration to determine if the operating system alerts an MDM or IDPS when it has detected an integrity check failure. Review MDM and IDPS logs to verify such reporting is occurring, perhaps forcing an integrity failure if one does not appear in the audit record. If the operating system is not configured to alert an MDM or IDPS in the event of an integrity failure, this is a finding. |
| 128 | The mobile operating system must support the capability of Mobile Device Management (MDM) system to detect when the device has been jailbroken or rooted. | Successful incident response and auditing relies on timely, accurate system information and analysis in order to allow the organization to identify and respond to potential incidents in a proficient manner. The ability of an MDM to detect jailbreaking or rooting device mitigates the potential for these breaches to have further consequences to the enterprise. | NIST SP 800-53, Rev3: SI-4 (12) | Review system documentation to determine that the MDM is able to detect when a device has been jailbroken or rooted. Review MDM logs to determine if it is capturing jailbroken or rooting events. If this detection does not occur, this is a finding. |
| 129 | The operating system must provide notification to an external device of failed automated security tests. | Automated security tests are critical in the detection of security attacks. Such checks include verification of the integrity of operating system files, device drivers, and security enforcement mechanisms. However, users and systems administrators can only benefit from the security tests of they are notified in case of failure. A notification mechanism reduces the risk that a security breach will go undetected. | NIST SP 800-53, Rev3: SI-6 (1) | Review system documentation and operating system configuration to determine how the operating system responds in the event of a failed automated security test. If the device is integrated with an MDM that is able to access device logs, then review system logs to determine if the operating system has provided notification of a failed automated security test. Otherwise, determine if there is some form of beaconing or alerting that could be detectable by an MDM or other network management system. If higher assurance is required, perform an action that would cause the device to fail an automated security test (e.g., insert an unknown SD card), and verify the operating system provides notification of the failure. If there are any known security tests for which notification does not occur, this is a finding. |
| 130 | The mobile operating system must conduct a device integrity scan at least once every six hours. | Unauthorized changes to the operating system software or information on the system can possibly result in integrity or availability concerns. In order to quickly react to this situation, the operating system must detect these changes. One aspect of detection is the frequency at which the scans occur. The ability to set an appropriate frequency mitigates the risk that an attack will go without detection longer than the scanning interval. | NIST SP 800-53, Rev3: SI-7 | Review the operating system and MDM agent software settings to verify the device integrity validation scan frequency is at least once every six hours. If it is not, this is a finding. |
| 131 | The mobile operating system verifies the integrity of all operating system files, device drivers, and security enforcement mechanisms at startup and at least every six hours thereafter using one or more DOS approved cryptographic mechanisms that compare attributes of the operating system configuration to a known good baseline. | One of the most significant indicators of a security attack is modification of operating system files, device drivers, or security enforcement mechanisms. An integrity verification capability or tool detects unauthorized modifications to files or permissions and either prevents further operation or reports its findings so an appropriate response can occur. | NIST SP 800-53, Rev3: SI-7 | Review system documentation, operating system configuration, and other security information resources to determine if the mobile operating system verifies the integrity of all operating system files, device drivers, and security enforcement mechanisms at startup and periodically thereafter using one or more DOS approved cryptographic mechanisms that compare attributes of the operating system configuration to a known good baseline. If such a capability is not embedded in the operating system, then the device must integrate a DOS approved tool providing this functionality. In this case, on a sample of devices, inspect the device to determine if an active system scanning integrity capability or tool is resident on the device. Validate the capability has been deemed acceptable for use within DOS. If the capability is not present or is inadequate, this is a finding. |
| 132 | The mobile operating system must be configured to only allow passwords composed of characters from at least three of the following four groups: | Password complexity or strength refers to how difficult it is to determine a password using a dictionary or brute force attack. Requiring more types of characters increases the password complexity, and therefore makes it more difficult for an adversary to discover the password. | NIST SP 800-53, Rev3: IA-5 (1) (a) | Review the password complexity configuration settings to determine if the requirement is met. If these are not available, attempt to reset the password to one that is non-compliant and verify the operating system rejects it. If the operating system permits a non-compliant device unlock password, this is a finding. |
|  |  |
| (a) Upper case letters (A-Z); | DOS 12 FAM 623.3-1 (A) (2) |
| (b) Lower case letters (a-z); |  |
| (c) Arabic numerals (0 through 9); and |  |
| (d) Nonalphanumeric characters (punctuation symbols). |  |
| 133 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable Wi-Fi connectivity. | All active wireless interfaces on a device pose a potential vulnerability to the system. An adversary may learn of new vulnerabilities in communications protocols or in the implementation of those protocols for which the system does not have defenses. | NIST SP 800-53, Rev4: AC-18 | Review system documentation and operating system documentation to determine if a systems administrator can disable the Wi-Fi connectivity interface. The system administrator may accomplish this functionality using an MDM. If a systems administrator cannot disable Wi-Fi connectivity, this is a finding. |
| 134 | The mobile device must enable the Secure Boot function. | The Secure Boot protocol uses Public Key Infrastructure (PKI) to authenticate images that load during the boot process. If secure boot protocol is enabled, the digital signing keys for the legitimate operating system(s) are installed in the firmware. The secure boot protocol checks, when software is loaded, to ensure that it has been signed by one of the keys that are installed. If Secure Boot is enabled, each time a system’s power is turned on or reset, the firmware checks the hardware peripherals and checks the operating system loaders’ certificates for a match in the database of “allowed” components that the OEM stores in the firmware. | NIST SP 800-53, Rev3: CM-6 (1) | This requirement would not allow the device to boot up normally if it has been tampered with. |
| 135 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable biometric authentication. | At this time, no biometric reader has been approved for Department of State use on mobile devices. This technology would allow unauthorized users to have access to Department of State sensitive data if compromised. By not permitting the use of biometric authentication, Department of State users are forced to use passcodes that meet Department of State passcode requirements. DS/Cybersecurity is aware of a vulnerability with the biometric readers that allow a malicious actor to easily recreate biometric data allowing for the successful bypass of the authentication mechanism. | NIST SP 800-53, Rev3: CM-6 (1) | Currently this includes TouchID on iOS devices and face recognition scanning on Android devices. |
| 136 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable cloud backup features. | A cloud backup feature may gather user's information such as PII, or sensitive documents. With this feature enabled, sensitive information will be backed up to the manufacturer's servers and database. This data is stored at a location which has unauthorized employees accessing this data. This data is stored on a server which has an unknown location to the Department of State. Disabling this feature mitigates the risk of a backup feature that stores sensitive data on a server which has the ability to be located in a country other than the United States. Mobile cloud providers have not undergone the proper evaluation and certification through IRM/IA and DS/CS for utilization at the Department of State. | NIST SP 800-53, Rev3: CM-6 (1) |  |
| 137 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable password keychains. | A password keychain is a function that will store users' account names and passwords in the cloud, then sync this data between the users' devices. An adversary may use any of the stored keychain passwords after unlocking one of the synchronized devices. If a user is synchronizing devices, the user must protect all of the devices to prevent unauthorized use of the passcodes. Moreover, the keychain being transmitted through the cloud opens the possibility that a well-resourced, sophisticated adversary could compromise the cloud-transmitted keychain. Not allowing the password keychain feature mitigates the risk of the encrypted set of passwords being compromised by being transmitted through the cloud or synchronized across multiple devices. Mobile cloud providers have not undergone the proper evaluation and certification through IRM/IA and DS/CS for utilization at the Department of State. | NIST SP 800-53, Rev3: CM-6 (1) |  |
| 138 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable Multimedia Messaging (MMS). | DS/SI/CS has identified vulnerabilities that may be exposed through the MMS feature, thus, DS/SI/CS has required that the IT policy be set to ‘Disabled’. | NIST SP 800-53, Rev3: CM-6 (1) |  |
| 139 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable voice assistant capabilities. | To prevent accidental exposure of SBU / classified data sent from the device to be processed on a server in an unknown location to the Department of State. Disabling this feature mitigates the risk of data being stored on a server which has the ability to be located in a country other than the United States. Mobile cloud providers have not undergone the proper evaluation and certification through IRM/IA and DS/CS for utilization at the Department of State. | NIST SP 800-53, Rev3: CM-6 (1) |  |
| 140 | The mobile operating system must provide the ability for a Mobile Device Management Solution (MDM) to disable the NFC protocol stack. | All active wireless interfaces on a device pose a potential vulnerability to the system. An adversary may learn of new vulnerabilities in communications protocols or in the implementation of those protocols for which the system does not have defenses. If an organization has reason to believe that the NFC stack is vulnerable, or learns of a vulnerability that cannot be immediately corrected, then disabling the NFC stack is an effective means to mitigate the risk. | NIST SP 800-53, Rev4: AC-18 | Review system documentation and operating system documentation to determine if a systems administrator can disable the NFC protocol stack. The system administrator may accomplish this functionality using an MDM. If a systems administrator cannot disable the NFC protocol stack, this is a finding. |

1. Appendix B: List of International Service Locations (subject to change)

| Bureau Symbol | Post Name | City | Country | Region |
| --- | --- | --- | --- | --- |
| AF | Embassy Luanda | Luanda | Angola | Africa |
| AF | Embassy Cotonou | Cotonou | Benin | Africa |
| AF | Embassy Gaborone | Gaborone | Botswana | Africa |
| AF | Embassy Ouagadougou | Ouagadougou | Burkina Faso | Africa |
| AF | Embassy Bujumbura | Bujumbura | Burundi | Africa |
| AF | Embassy Praia | Praia | Cabo Verde | Africa |
| AF | Embassy Branch Office Douala | Douala | Cameroon | Africa |
| AF | Embassy Yaounde | Yaounde | Cameroon | Africa |
| AF | Embassy Bangui | Bangui | Central African Republic | Africa |
| AF | Embassy N’Djamena | N’Djamena | Chad | Africa |
| AF | Embassy Brazzaville | Brazzaville | Congo (Brazzaville) | Africa |
| AF | Embassy Kinshasa | Kinshasa | Congo (Kinshasa) | Africa |
| AF | Embassy Abidjan | Abidjan | Côte d’Ivoire | Africa |
| AF | Embassy Djibouti | Djibouti | Djibouti | Africa |
| AF | Embassy Malabo | Malabo | Equatorial Guinea | Africa |
| AF | Embassy Asmara | Asmara | Eritrea | Africa |
| AF | Embassy Addis Ababa | Addis Ababa | Ethiopia | Africa |
| AF | U.S. Mission to the African Union, Addis Ababa | Addis Ababa | Ethiopia | Africa |
| AF | Embassy Libreville | Libreville | Gabon | Africa |
| AF | Embassy Banjul | Banjul | Gambia, The | Africa |
| AF | Embassy Accra | Accra | Ghana | Africa |
| AF | Embassy Conakry | Conakry | Guinea | Africa |
| AF | Embassy Nairobi | Nairobi | Kenya | Africa |
| AF | U.S. Embassy to Sudan, in Nairobi | Nairobi | Kenya | Africa |
| AF | U.S. Mission to UNEP and UN-HABITAT (USUNEP/UN-HABITAT), Nairobi | Nairobi | Kenya | Africa |
| AF | Embassy Maseru | Maseru | Lesotho | Africa |
| AF | Embassy Monrovia | Monrovia | Liberia | Africa |
| AF | Embassy Antananarivo | Antananarivo | Madagascar | Africa |
| AF | Embassy Lilongwe | Lilongwe | Malawi | Africa |
| AF | Embassy Bamako | Bamako | Mali | Africa |
| AF | Embassy Nouakchott | Nouakchott | Mauritania | Africa |
| AF | Embassy Port Louis | Port Louis | Mauritius | Africa |
| AF | Embassy Maputo | Maputo | Mozambique | Africa |
| AF | Embassy Windhoek | Windhoek | Namibia | Africa |
| AF | Embassy Niamey | Niamey | Niger | Africa |
| AF | Embassy Abuja | Abuja | Nigeria | Africa |
| AF | Consulate General Lagos | Lagos | Nigeria | Africa |
| AF | Embassy Kigali | Kigali | Rwanda | Africa |
| AF | Embassy Dakar | Dakar | Senegal | Africa |
| AF | Embassy Freetown | Freetown | Sierra Leone | Africa |
| AF | Embassy Mogadishu | Mogadishu | Somalia | Africa |
| AF | Consulate General Cape Town | Cape Town | South Africa | Africa |
| AF | Consulate General Durban | Durban | South Africa | Africa |
| AF | Consulate General Johannesburg | Johannesburg | South Africa | Africa |
| AF | Embassy Pretoria | Pretoria | South Africa | Africa |
| AF | Embassy Juba | Juba | South Sudan | Africa |
| AF | Juba | Juba | Sudan | Africa |
| AF | Embassy Khartoum | Khartoum | Sudan | Africa |
| AF | Embassy Mbabane | Mbabane | Swaziland | Africa |
| AF | Embassy Dar es Salaam | Dar es Salaam | Tanzania | Africa |
| AF | Embassy Lome | Lome | Togo | Africa |
| AF | Embassy Kampala | Kampala | Uganda | Africa |
| AF | Embassy Lusaka | Lusaka | Zambia | Africa |
| AF | Embassy Harare | Harare | Zimbabwe | Africa |
| EAP | Embassy Canberra | Canberra | Australia | East Asia Pacific |
| EAP | Consulate General Melbourne | Melbourne | Australia | East Asia Pacific |
| EAP | Consulate General Perth | Perth | Australia | East Asia Pacific |
| EAP | Consulate General Sydney | Sydney | Australia | East Asia Pacific |
| EAP | Embassy Bandar Seri Begawan | Bandar Seri Begawan | Brunei | East Asia Pacific |
| EAP | Embassy Rangoon | Rangoon | Burma | East Asia Pacific |
| EAP | Embassy Phnom Penh | Phnom Penh | Cambodia | East Asia Pacific |
| EAP | Embassy Beijing | Beijing | China | East Asia Pacific |
| EAP | Consulate General Chengdu | Chengdu | China | East Asia Pacific |
| EAP | Consulate General Guangzhou | Guangzhou | China | East Asia Pacific |
| EAP | Consulate General Shanghai | Shanghai | China | East Asia Pacific |
| EAP | Consulate General Shenyang | Shenyang | China | East Asia Pacific |
| EAP | Consulate General Wuhan | Wuhan | China | East Asia Pacific |
| EAP | Embassy Suva | Suva | Fiji | East Asia Pacific |
| EAP | Consulate General Hong Kong | Hong Kong | Hong Kong | East Asia Pacific |
| EAP | Embassy Jakarta | Jakarta | Indonesia | East Asia Pacific |
| EAP | U.S. Mission to the Association of South East Asian Nations (ASEAN), Jakarta | Jakarta | Indonesia | East Asia Pacific |
| EAP | Consulate Medan | Medan | Indonesia | East Asia Pacific |
| EAP | Consulate General Surabaya | Surabaya | Indonesia | East Asia Pacific |
| EAP | Consulate Fukuoka | Fukuoka | Japan | East Asia Pacific |
| EAP | Consulate Nagoya | Nagoya | Japan | East Asia Pacific |
| EAP | Consulate General Naha, Okinawa | Naha | Japan | East Asia Pacific |
| EAP | Consulate General Osaka-Kobe | Osaka | Japan | East Asia Pacific |
| EAP | Consulate General Sapporo | Sapporo | Japan | East Asia Pacific |
| EAP | Embassy Tokyo | Tokyo | Japan | East Asia Pacific |
| EAP | Consulate Busan | Busan | Korea, South | East Asia Pacific |
| EAP | Embassy Seoul | Seoul | Korea, South | East Asia Pacific |
| EAP | Embassy Vientiane | Vientiane | Laos | East Asia Pacific |
| EAP | Embassy Kuala Lumpur | Kuala Lumpur | Malaysia | East Asia Pacific |
| EAP | Embassy Majuro | Majuro | Marshall Islands | East Asia Pacific |
| EAP | Embassy Kolonia | Kolonia | Micronesia, Federated States of | East Asia Pacific |
| EAP | Embassy Ulaanbaatar | Ulaanbaatar | Mongolia | East Asia Pacific |
| EAP | Consulate General Auckland | Auckland | New Zealand | East Asia Pacific |
| EAP | Embassy Wellington | Wellington | New Zealand | East Asia Pacific |
| EAP | Embassy Koror | Koror | Palau | East Asia Pacific |
| EAP | Embassy Port Moresby | Port Moresby | Papua New Guinea | East Asia Pacific |
| EAP | Embassy Manila | Manila | Philippines | East Asia Pacific |
| EAP | Embassy Apia | Apia | Samoa | East Asia Pacific |
| EAP | Embassy Singapore | Singapore | Singapore | East Asia Pacific |
| EAP | American Institute in Taiwan in Kaohsiung | Kaohsiung | Taiwan | East Asia Pacific |
| EAP | American Institute in Taiwan in Taipei | Taipei | Taiwan | East Asia Pacific |
| EAP | Embassy Taipei | Taipei | Taiwan | East Asia Pacific |
| EAP | Embassy Bangkok | Bangkok | Thailand | East Asia Pacific |
| EAP | Consulate General Chiang Mai | Chiang Mai | Thailand | East Asia Pacific |
| EAP | Embassy Dili | Dili | Timor-Leste | East Asia Pacific |
| EAP | Embassy Hanoi | Hanoi | Vietnam | East Asia Pacific |
| EAP | Consulate General Ho Chi Minh City | Ho Chi Minh City | Vietnam | East Asia Pacific |
| EB | U.S. Mission to the Organization for Economic Cooperation and Development, Paris | Paris | France | Europe & Eurasia |
| EUR | Embassy Tirana | Tirana | Albania | Europe & Eurasia |
| EUR | Embassy Yerevan | Yerevan | Armenia | Europe & Eurasia |
| EUR | U.S. Mission to the Organization for Security and Cooperation in Europe, Vienna | Vienna | Austria | Europe & Eurasia |
| EUR | Embassy Vienna | Vienna | Austria | Europe & Eurasia |
| EUR | Embassy Baku | Baku | Azerbaijan | Europe & Eurasia |
| EUR | Embassy Minsk | Minsk | Belarus | Europe & Eurasia |
| EUR | Embassy Brussels | Brussels | Belgium | Europe & Eurasia |
| EUR | U.S. Mission to the European Union (USEU), Brussels | Brussels | Belgium | Europe & Eurasia |
| EUR | U.S. Mission to the North Atlantic Treaty Organization (USNATO), Brussels | Brussels | Belgium | Europe & Eurasia |
| EUR | Embassy Branch Office Banja Luka | Banja Luka | Bosnia and Herzegovina | Europe & Eurasia |
| EUR | Embassy Branch Office Mostar | Mostar | Bosnia and Herzegovina | Europe & Eurasia |
| EUR | Embassy Sarajevo | Sarajevo | Bosnia and Herzegovina | Europe & Eurasia |
| EUR | Embassy Sofia | Sofia | Bulgaria | Europe & Eurasia |
| EUR | Embassy Zagreb | Zagreb | Croatia | Europe & Eurasia |
| EUR | Embassy Nicosia | Nicosia | Cyprus | Europe & Eurasia |
| EUR | Embassy Prague | Prague | Czech Republic | Europe & Eurasia |
| EUR | Embassy Copenhagen | Copenhagen | Denmark | Europe & Eurasia |
| EUR | Embassy Tallinn | Tallinn | Estonia | Europe & Eurasia |
| EUR | Embassy Helsinki | Helsinki | Finland | Europe & Eurasia |
| EUR | Consulate Bordeaux | Bordeaux | France | Europe & Eurasia |
| EUR | Consulate Lyon | Lyon | France | Europe & Eurasia |
| EUR | Consulate General Marseille | Marseille | France | Europe & Eurasia |
| EUR | Embassy Paris | Paris | France | Europe & Eurasia |
| EUR | Consulate Rennes | Rennes | France | Europe & Eurasia |
| EUR | Consulate General Strasbourg | Strasbourg | France | Europe & Eurasia |
| EUR | Consulate Toulouse | Toulouse | France | Europe & Eurasia |
| EUR | Embassy Tbilisi | Tbilisi | Georgia | Europe & Eurasia |
| EUR | Embassy Berlin | Berlin | Germany | Europe & Eurasia |
| EUR | Consulate General Dusseldorf | Dusseldorf | Germany | Europe & Eurasia |
| EUR | Consulate General Frankfurt Am Main | Frankfurt am Main | Germany | Europe & Eurasia |
| EUR | Consulate General Hamburg | Hamburg | Germany | Europe & Eurasia |
| EUR | Consulate General Leipzig | Leipzig | Germany | Europe & Eurasia |
| EUR | Consulate General Munich | Munchen | Germany | Europe & Eurasia |
| EUR | Embassy Athens | Athens | Greece | Europe & Eurasia |
| EUR | Consulate General Thessaloniki | Thessaloniki | Greece | Europe & Eurasia |
| EUR | Embassy Budapest | Budapest | Hungary | Europe & Eurasia |
| EUR | Embassy Reykjavik | Reykjavik | Iceland | Europe & Eurasia |
| EUR | Embassy Dublin | Dublin | Ireland | Europe & Eurasia |
| EUR | Consulate General Florence | Florence | Italy | Europe & Eurasia |
| EUR | Consulate General Milan | Milan | Italy | Europe & Eurasia |
| EUR | Consulate General Naples | Naples | Italy | Europe & Eurasia |
| EUR | Embassy Rome | Rome | Italy | Europe & Eurasia |
| EUR | Embassy Pristina | Pristina | Kosovo | Europe & Eurasia |
| EUR | Embassy Riga | Riga | Latvia | Europe & Eurasia |
| EUR | Embassy Vilnius | Vilnius | Lithuania | Europe & Eurasia |
| EUR | Embassy Luxembourg | Luxembourg | Luxembourg | Europe & Eurasia |
| EUR | Embassy Skopje | Skopje | Macedonia | Europe & Eurasia |
| EUR | Embassy Valletta | Valletta | Malta | Europe & Eurasia |
| EUR | Embassy Chisinau | Chisinau | Moldova | Europe & Eurasia |
| EUR | Embassy Podgorica | Podgorica | Montenegro | Europe & Eurasia |
| EUR | Consulate General Amsterdam | Amsterdam | Netherlands | Europe & Eurasia |
| EUR | Embassy The Hague | The Hague | Netherlands | Europe & Eurasia |
| EUR | Embassy Oslo | Oslo | Norway | Europe & Eurasia |
| EUR | Consulate General Krakow | Krakow | Poland | Europe & Eurasia |
| EUR | Embassy Warsaw | Warsaw | Poland | Europe & Eurasia |
| EUR | Embassy Lisbon | Lisbon | Portugal | Europe & Eurasia |
| EUR | Consulate Ponta Delgada, Sao Miguel, Azores | Ponta Delgada | Portugal | Europe & Eurasia |
| EUR | Embassy Bucharest | Bucharest | Romania | Europe & Eurasia |
| EUR | Embassy Moscow | Moscow | Russia | Europe & Eurasia |
| EUR | Consulate General St. Petersburg | Saint Petersburg | Russia | Europe & Eurasia |
| EUR | Consulate General Vladivostok | Vladivostok | Russia | Europe & Eurasia |
| EUR | Consulate General Yekaterinburg | Yekaterinburg | Russia | Europe & Eurasia |
| EUR | Embassy Belgrade | Belgrade | Serbia | Europe & Eurasia |
| EUR | Embassy Bratislava | Bratislava | Slovakia | Europe & Eurasia |
| EUR | Embassy Ljubljana | Ljubljana | Slovenia | Europe & Eurasia |
| EUR | Consulate General Barcelona | Barcelona | Spain | Europe & Eurasia |
| EUR | Embassy Madrid | Madrid | Spain | Europe & Eurasia |
| EUR | Embassy Stockholm | Stockholm | Sweden | Europe & Eurasia |
| EUR | Embassy Bern | Bern | Switzerland | Europe & Eurasia |
| EUR | Consulate Adana | Adana | Turkey | Europe & Eurasia |
| EUR | Embassy Ankara | Ankara | Turkey | Europe & Eurasia |
| EUR | Consulate General Istanbul | Istanbul | Turkey | Europe & Eurasia |
| EUR | Embassy Kyiv | Kyiv | Ukraine | Europe & Eurasia |
| EUR | Consulate General Belfast, Northern Ireland | Belfast | United Kingdom | Europe & Eurasia |
| EUR | Consulate General Edinburgh, Scotland | Edinburgh | United Kingdom | Europe & Eurasia |
| EUR | Embassy London, England | London | United Kingdom | Europe & Eurasia |
| EUR | Embassy Vatican City | Vatican City | Vatican City | Europe & Eurasia |
| EUR | Consulate General Hamilton | Hamilton | Bermuda | Western Hemisphere |
| IO | U.S. Mission to U.N. System Organizations in Vienna, Vienna | Vienna | Austria | Europe & Eurasia |
| IO | U.S. Mission to UNESCO, Paris | Paris | France | Europe & Eurasia |
| IO | U.S. Mission to the UN Agencies, Rome | Rome | Italy | Europe & Eurasia |
| IO | U.S. Mission, Geneva | Geneva | Switzerland | Europe & Eurasia |
| IO | U.S. Mission to the United Nations, New York | New York | United States | USA & US Territories |
| IO | U.S. Mission to the International Civil Aviation Organization (USICAO), Montreal | Montreal | Canada | Western Hemisphere |
| NEA | Embassy Algiers | Algiers | Algeria | Near East |
| NEA | Embassy Manama | Manama | Bahrain | Near East |
| NEA | Consulate General Alexandria | Alexandria | Egypt | Near East |
| NEA | Embassy Cairo | Cairo | Egypt | Near East |
| NEA | Embassy Tehran | Tehran | Iran | Near East |
| NEA | Consulate General Basrah | Al Basrah | Iraq | Near East |
| NEA | Embassy Baghdad | Baghdad | Iraq | Near East |
| NEA | Consulate General Erbil | Kirkuk | Iraq | Near East |
| NEA | Consulate General Kirkuk | Kirkuk | Iraq | Near East |
| NEA | Embassy Tel Aviv | Tel Aviv | Israel | Near East |
| NEA | Consulate General Jerusalem | Jerusalem | Jerusalem | Near East |
| NEA | Embassy Amman | Amman | Jordan | Near East |
| NEA | Embassy Kuwait | Kuwait City | Kuwait | Near East |
| NEA | Embassy Beirut | Beirut | Lebanon | Near East |
| NEA | Embassy Tripoli | Tripoli | Libya | Near East |
| NEA | Consulate General Casablanca | Casablanca | Morocco | Near East |
| NEA | Embassy Rabat | Rabat | Morocco | Near East |
| NEA | Embassy Muscat | Muscat | Oman | Near East |
| NEA | Embassy Doha | Doha | Qatar | Near East |
| NEA | Consulate General Dhahran | Dhahran | Saudi Arabia | Near East |
| NEA | Consulate General Jeddah | Jeddah | Saudi Arabia | Near East |
| NEA | Embassy Riyadh | Riyadh | Saudi Arabia | Near East |
| NEA | Embassy Damascus | Damascus | Syria | Near East |
| NEA | Embassy Tunis | Tunis | Tunisia | Near East |
| NEA | Embassy Abu Dhabi | Abu Dhabi | United Arab Emirates | Near East |
| NEA | Consulate General Dubai | Dubai | United Arab Emirates | Near East |
| NEA | Embassy Sanaa | Sanaa | Yemen | Near East |
| SCA | Consulate Herat | Herat | Afghanistan | South & Central Asia |
| SCA | Embassy Kabul | Kabul | Afghanistan | South & Central Asia |
| SCA | Consulate Mazar-e Sharif | Mazar-e Sharif | Afghanistan | South & Central Asia |
| SCA | Embassy Dhaka | Dhaka | Bangladesh | South & Central Asia |
| SCA | Consulate General Chennai | Chennai | India | South & Central Asia |
| SCA | Consulate General Hyderabad | Hyderabad | India | South & Central Asia |
| SCA | Consulate General Kolkata | Kolkata | India | South & Central Asia |
| SCA | Consulate General Mumbai | Mumbai | India | South & Central Asia |
| SCA | Embassy New Delhi | New Delhi | India | South & Central Asia |
| SCA | Almaty Consulate General, in Kazakhstan | Almaty | Kazakhstan | South & Central Asia |
| SCA | U.S. Embassy to Tajikistan, in Almaty | Almaty | Kazakhstan | South & Central Asia |
| SCA | Embassy Astana | Astana | Kazakhstan | South & Central Asia |
| SCA | Embassy Bishkek | Bishkek | Kyrgyzstan | South & Central Asia |
| SCA | Embassy Kathmandu | Kathmandu | Nepal | South & Central Asia |
| SCA | Embassy Islamabad | Islamabad | Pakistan | South & Central Asia |
| SCA | Consulate General Karachi | Karachi | Pakistan | South & Central Asia |
| SCA | Consulate General Lahore | Lahore | Pakistan | South & Central Asia |
| SCA | Consulate General Peshawar | Peshawar | Pakistan | South & Central Asia |
| SCA | Embassy Colombo | Colombo | Sri Lanka | South & Central Asia |
| SCA | Embassy Dushanbe | Dushanbe | Tajikistan | South & Central Asia |
| SCA | Embassy Ashgabat | Ashgabat | Turkmenistan | South & Central Asia |
| SCA | Embassy Tashkent | Tashkent | Uzbekistan | South & Central Asia |
| WHA | U.S. Mission to the Organization of American States, Washington, D.C. | Washington | United States | USA & US Territories |
| WHA | Embassy Buenos Aires | Buenos Aires | Argentina | Western Hemisphere |
| WHA | Embassy Nassau | Nassau | Bahamas, The | Western Hemisphere |
| WHA | Embassy Bridgetown | Bridgetown | Barbados | Western Hemisphere |
| WHA | Embassy Belmopan | Belmopan | Belize | Western Hemisphere |
| WHA | Embassy La Paz | La Paz | Bolivia | Western Hemisphere |
| WHA | Embassy Brasilia | Brasilia | Brazil | Western Hemisphere |
| WHA | Consulate General Recife | Recife | Brazil | Western Hemisphere |
| WHA | Consulate General Rio de Janeiro | Rio de Janeiro | Brazil | Western Hemisphere |
| WHA | Consulate General Sao Paulo | Sao Paulo | Brazil | Western Hemisphere |
| WHA | Consulate General Calgary, Alberta | Calgary | Canada | Western Hemisphere |
| WHA | Consulate General Halifax, Nova Scotia | Halifax | Canada | Western Hemisphere |
| WHA | Consulate General Montreal, Quebec | Montreal | Canada | Western Hemisphere |
| WHA | Embassy Ottawa, Ontario | Ottawa | Canada | Western Hemisphere |
| WHA | Consulate General Quebec, Quebec | Quebec | Canada | Western Hemisphere |
| WHA | Consulate General Toronto, Ontario | Toronto | Canada | Western Hemisphere |
| WHA | Consulate General Vancouver, British Columbia | Vancouver | Canada | Western Hemisphere |
| WHA | Consulate Winnipeg, Manitoba | Winnipeg | Canada | Western Hemisphere |
| WHA | Embassy Santiago | Santiago | Chile | Western Hemisphere |
| WHA | Embassy Bogota | Bogota | Colombia | Western Hemisphere |
| WHA | Embassy Branch Office Cartagena | Cartagena | Colombia | Western Hemisphere |
| WHA | Embassy San Jose | San Jose | Costa Rica | Western Hemisphere |
| WHA | USINT Havana | Havana | Cuba | Western Hemisphere |
| WHA | U.S. Embassy Havana | Havana | Cuba | Western Hemisphere |
| WHA | Consulate General Curacao | Curacao | Curacao | Western Hemisphere |
| WHA | Embassy Santo Domingo | Santo Domingo | Dominican Republic | Western Hemisphere |
| WHA | Consulate General Guayaquil | Guayaquil | Ecuador | Western Hemisphere |
| WHA | Embassy Quito | Quito | Ecuador | Western Hemisphere |
| WHA | Embassy San Salvador | San Salvador | El Salvador | Western Hemisphere |
| WHA | Embassy St. George’s | Saint George’s | Grenada | Western Hemisphere |
| WHA | Embassy Guatemala City | Guatemala City | Guatemala | Western Hemisphere |
| WHA | Embassy Georgetown | Georgetown | Guyana | Western Hemisphere |
| WHA | Embassy Port au Prince | Port-au-Prince | Haiti | Western Hemisphere |
| WHA | Embassy Tegucigalpa | Tegucigalpa | Honduras | Western Hemisphere |
| WHA | Embassy Kingston | Kingston | Jamaica | Western Hemisphere |
| WHA | Consulate General Ciudad Juarez | Ciudad Juarez | Mexico | Western Hemisphere |
| WHA | Consulate General Guadalajara | Guadalajara | Mexico | Western Hemisphere |
| WHA | Consulate General Hermosillo | Hermosillo | Mexico | Western Hemisphere |
| WHA | Consulate General Matamoros | Matamoros | Mexico | Western Hemisphere |
| WHA | Consulate General Merida | Merida | Mexico | Western Hemisphere |
| WHA | Embassy Mexico City | Mexico City | Mexico | Western Hemisphere |
| WHA | Consulate General Monterrey | Monterrey | Mexico | Western Hemisphere |
| WHA | Consulate General Nogales | Nogales | Mexico | Western Hemisphere |
| WHA | Consulate General Nuevo Laredo | Nuevo Laredo | Mexico | Western Hemisphere |
| WHA | Consulate General Tijuana | Tijuana | Mexico | Western Hemisphere |
| WHA | Embassy Managua | Managua | Nicaragua | Western Hemisphere |
| WHA | Embassy Panama City | Panama City | Panama | Western Hemisphere |
| WHA | Embassy Asuncion | Asuncion | Paraguay | Western Hemisphere |
| WHA | Embassy Lima | Lima | Peru | Western Hemisphere |
| WHA | Embassy Paramaribo | Paramaribo | Suriname | Western Hemisphere |
| WHA | Embassy Port of Spain | Port of Spain | Trinidad and Tobago | Western Hemisphere |
| WHA | Embassy Montevideo | Montevideo | Uruguay | Western Hemisphere |
| WHA | Embassy Caracas | Caracas | Venezuela | Western Hemisphere |