2017

Report to the President on Federal IT Modernization

Table of Contents

Preface

The United States is unparalleled in its commitment to protecting Americans' liberties and freedoms and is unmatched in its national security infrastructure. Hardworking Americans have built the world's largest economy and solved some of the world's greatest challenges through innovations in science and technology. It is imperative for the Federal Government to leverage these innovations to provide better service for its citizens in the most cost-effective and secure manner. This Administration has prioritized modernization of Federal information technology (IT) systems, and to that end, has committed to help agencies better leverage American innovations through increased use of commercial technology.

As a demonstration of this commitment, on May 1, 2017, the President established the American Technology Council (ATC) to effectuate the secure and efficient use of IT across the Federal Government.[1] Just days later, on May 11, 2017, the President signed Executive Order (EO) 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.[2] The latter EO tasks the Director of ATC to coordinate a report to the President from the Secretary of the Department of Homeland Security (DHS), the Director of the Office of Management and Budget (OMB), and the Administrator of the General Services Administration (GSA), in consultation with the Secretary of Commerce (Commerce), regarding the modernization of Federal IT.

Acknowledging that Federal agencies are still working, and must continue to work, to meet the objectives of other critical modernization initiatives – for instance, by automating their manual processes, implementing new and diverse testing and scanning options, deploying patches both responsively and preventatively, and by transitioning away from unsupported software – this report outlines the current and envisioned state of Federal IT, and it provides specific recommendations to jumpstart a new wave of modernization efforts.

This report is focused on modernization efforts to improve the security posture of Federal IT. Though this covers a significant footprint of modernization needs, the public comment period generated responses from industry that highlighted the importance of providing an overarching IT modernization plan, which aligns these efforts with ongoing work to improve citizen-facing services, make better use of mobile technologies, improving security across the Federal enterprise, and other key efforts. In response to this, the American Technology Council will provide this amplifying context following publication of this final report.

The enclosed plan incorporates the efforts of key Government stakeholders in identifying ways for the Government to enhance its cybersecurity posture, modernize the Federal IT enterprise, and create a more robust partnership between Government and industry. Additionally, the ATC has convened top private and public sector leaders to elicit and incorporate input on the vision for the future of Federal IT, and it intends to seek further input to ensure successful implementation of modernization recommendations.

---

[1] *Presidential Executive Order on the Establishment of the American Technology Council*. May 2017.

[2] *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. May 2017.

Executive Summary

This report outlines a vision and recommendations for the Federal Government to build a more modern and secure architecture for Federal IT systems.[3] Agencies have attempted to modernize their systems but have been stymied by a variety of factors, including resource prioritization, ability to procure services quickly, and technical issues. Recommendations to address the aforementioned issues are grouped into two categories of effort: the modernization and consolidation of networks and the use of shared services to enable future network architectures. In addition to specific recommendations, this report outlines an agile process for updating policies and reference architectures to help the Government more rapidly leverage American innovation.

Network Modernization and Consolidation. This report envisions a modern Federal IT architecture where agencies are able to maximize secure use of cloud computing, modernize Government-hosted applications, and securely maintain legacy systems. Specific actions in this report focus on the first two areas, where securely maintaining legacy systems is addressed in other areas of EO 13800. These actions enable agencies to move from protection of their network perimeters and managing legacy physical deployments toward protection of Federal data and cloud-optimized deployments. The report also emphasizes a risk-based approach that focuses agency resources on their highest value assets, per OMB's authorities provided by the Federal Information Security Modernization Act of 2014 (FISMA)[4] and OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The report addresses current impediments or obstacles to adopting modernized cloud technologies by piloting new implementation approaches, and using these test cases to inform rapid policy updates. The report also focuses on consolidating and improving acquisition of network services so that management of security services for networks are consolidated where possible and managed to high standards. Specific actions include:

1. **Prioritize the Modernization of High-Risk High Value Assets (HVAs).** Prioritize modernization of legacy IT by focusing on enhancement of security and privacy controls for those assets that are essential for Federal agencies to serve the American people and whose security posture is most vulnerable.

2. **Modernize the Trusted Internet Connections (TIC) and National Cybersecurity Protection System (NCPS) Program to Enable Cloud Migration.** Use real world implementation test cases to identify solutions to current barriers regarding agency cloud adoption. Update relevant network security policies and architectures to enable agencies to focus on both network and data-level security and privacy, while ensuring incident detection and prevention capabilities are modernized to address the latest threats.

3. **Consolidate Network Acquisitions and Management.** Consolidate and standardize network and security service acquisition to take full advantage of economies of scale, while minimizing duplicative investments in existing security capabilities.

---

[3] Not to include national security systems as defined in Section 3552(b)(6) of Title 44, United States Code.

[4] *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, 128 Stat. 3073), as amended.

Shared Services to Enable Future Network Architectures. The following section of this report lays out an approach to enable, with ongoing Government-wide category management efforts, the Federal Government to shift toward a consolidated IT model by adopting centralized offerings for commodity IT. The recommendations detail steps to address current impediments in policy, resource allocation, and agency prioritization to enabling the use of cloud, collaboration tools, and other security shared services. For the purposes of this Report and its implementation, shared services is the provision of consolidated capabilities or functions (services and/or IT systems) that are common across multiple agencies. Shared Services can enable agency efficiency by reducing duplication and costs through consistent delivery of standardized capabilities or functions in ways that make the most of innovative processes and commercial solutions. Specific actions include:

1. **Enable use of Commercial Cloud.** Improve contract vehicles to enable agencies to acquire commercial cloud products that meet Government standards.

2. **Accelerate Adoption of Cloud Email and Collaboration Tools.** Provide support for migration to cloud email and collaboration suites that leverage the Government's buying power. Define the next set of agencies to migrate to commercial email and collaboration suites.

3. **Improve Existing and Provide Additional Security Shared Services.** Provide consolidated capabilities that replace or augment existing agency-specific technology to improve both visibility and security.

Resourcing Federal Network IT Modernization. In order to implement the Federal IT modernization efforts outlined in this report, agencies will need to realign their IT resources appropriately using business-focused, data-driven analysis and technical evaluation. OMB will inform agencies that agency Chief Information Officers (CIOs) work with their Chief Financial Officers (CFOs) and Senior Agency Officials for Privacy (SAOPs), in consultation with OMB, to determine which of their systems will be prioritized for modernization, identifying strategies to reallocate resources appropriately. In accordance with the terms of agency contracts and consistent with law, agencies should consider evaluating ongoing and planned acquisitions that further develop or enhance legacy IT systems identified that need modernization to ensure consistency with broader IT strategies outlined in this report. Agencies should also emphasize reprioritizing funds and should consider "cut and invest" strategies that reallocate funding from obsolete legacy IT systems to modern technologies, cloud solutions, and shared services, using agile development practices and the best practices within GSA's Unified Shared Services' Modernization and Migration Management Framework,[5] where appropriate.

Taken together, these recommendations will modernize the security and functionality of Federal IT, allow the Federal Government to improve service delivery, and focus effort and resources on what is most important to customers of Government services.

[5] Introduction to Modernization and Migration Management (M3), Unified Shared Services Management.

Network Modernization & Consolidation

Summary of Efforts to Date

The Federal Government has engaged in several efforts to modernize existing IT systems, to improve processes for the acquisition and development of new solutions, and to restructure underlying frameworks for service and lifecycle management. The *E-Government Act of 2002* recognized the importance of a well-managed, modern, and secure Federal IT ecosystem, building upon concepts captured in the Clinger-Cohen Act, the *Paperwork Reduction Act*, and OMB Circular A-130, *Managing Information as a Strategic Resource*.[6] Additionally, the *Federal Information Security Management Act of 2002* and, subsequently, *the Federal Information Security Modernization Act of 2014,* serve as the governing authority for OMB to provide overall guidance and policy for Government-wide Federal cybersecurity.

Pursuant to these authorities, OMB established the IT Infrastructure Optimization Line of Business, which developed common Government-wide performance measures for service levels and costs, identified best practices, and provided guidance for agency IT infrastructure transition plans. An Enterprise Architecture and Centralizing Infrastructure was constructed some years later, and in 2010, the Federal Data Center Consolidation Initiative (FDCCI) directed agencies to inventory their data centers, develop consolidation plans, and assess virtual or cloud alternatives.[7]

Between the launch of the FDCCI and its conclusion in 2015, the Cloud First Initiative and the Federal Risk and Authorization Management Program (FedRAMP) were activated in 2011, with FedRAMP providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. Driven by the momentum of these and other efforts, in 2016 the Data Center Optimization Initiative arose as an update to the FDCCI based on requirements of the *Federal IT Acquisition Reform Act* (FITARA).[8] These efforts have helped agencies to begin modernizing their IT and this Report is intended to help resolve some of the impediments surfaced throughout implementation of those efforts and further accelerate Federal IT modernization.

Transitioning to consolidated network architectures and shared services requires consideration of how these products or services will be acquired. Current challenges associated with use of commercial acquisition practices limit the Federal Government's ability to achieve the modernization goals.

There are statutory and regulatory requirements that prevent the use of accepted commercial best acquisition practices. Changes and modifications to the existing acquisition requirements could be implemented to achieve efficiencies while maintaining the core tenet of fairness.

---

[6] *E-Government Act of 2002* (Pub. L. No. 107-347); *Information Technology Management Reform Act of 1996*, "Clinger-Cohen Act (CCA)," (Pub. L. 104-106, Division E); and *Paperwork Reduction Act of 1995* (Pub. L. No. 96-511).

[7] *State of Federal IT Report*, Public Release Version 1.0.

[8] *Federal IT Acquisition Reform Act* (included in the *National Defense Authorization Act for Fiscal Year 2015* – Pub. L. 113-291).

Current State

In recent years, Government-wide initiatives and policies have focused on the transition to a more efficient, more secure, and customer-focused IT environment. The preponderance of efforts to protect Federal IT systems to date have been focused at the network level. This drove agencies to consolidate human and technical resources around a limited number of connections and standardized physical access points, with the intent of producing more robust security management.

Current policy, agency prioritization, and associated investments prioritized through the budget process have emphasized perimeter network-based security protections. This is manifested most visibly through the Trusted Internet Connections (TIC) and National Cybersecurity Protection System (NCPS) programs.[9] This report recommends emphasizing a layered defensive strategy in Government-wide programs, through increasing emphasis on application and data-level protections. This shift in focus, coupled with lessons learned from the current implementation and advances in technology will drive strategic changes to the NCPS program, as described in Appendix C. It will also provide greater defense-in-depth capabilities that will help prevent malicious actors from moving laterally across linked networks to access large amounts of valuable information.

These well-intentioned initiatives have resulted in security implementations that negatively affect performance and create barriers to use of commercial technology. As an example, policy and existing implementation of enterprise cybersecurity tools drives the physical consolidation of all network traffic to and from Federal information systems. This hampers agencies' ability to acquire new technologies like commercial cloud, which rely on a distributed network model and emphasize optimization of virtual rather than physical controls of data. In this case, policies and supporting capabilities which require routing all traffic through a limited number of on premise access points not only impacts service performance and availability, but it also undermines the value proposition of a distributed cloud architecture and flexible mobile access to services.

Consequently, in order to successfully meet their mission and business objectives, agencies often circumvent network-based security protections to use commercial cloud. Another negative consequence of overreliance on network-based protections is the emergence of operational capability gaps at other levels, such as the data and application levels. This has resulted in

[9] The TIC and NCPS initiatives are further described in the Comprehensive National Cyber Security Initiative (CNCI), established by Joint Presidential Directive NSPD-54/HSPD-23; OMB Memorandum M-08-16, Guidance for TIC Statement of Capability Form (SOC); OMB Memorandum M-08-26, *Transition from FTS 2001 to Networx*; OMB Memorandum M-08-27, Guidance for TIC Compliance; OMB Memorandum M-09-32, *Update on the TIC Initiative*; and DHS's TIC Reference Architecture. These documents provide further details on agency, OMB, and DHS responsibilities and reporting requirements, acquisition vehicles, and technical capabilities under the TIC initiative. The *Homeland Security Act*, as amended by section 223 of the *Federal Cybersecurity Enhancement Act of 2015*, *Consolidated Appropriations Act of 2016* (Pub. L. No. 114-113, 129 Stat. 2242, Division N, Title II, Subtitle B), requires DHS to "deploy, operate, and maintain" and "make available for use by any agency" capabilities to detect cybersecurity risks in agency network traffic and take actions to mitigate those risks (6 U.S.C. § 151(b)(1)). DHS currently provides these capabilities through its NCPS program and, as required by law, ensures all retention, use, and disclosure of information obtained through NCPS occurs only for protecting information and information systems from cybersecurity risks (*See id.* § 151(c)(3)). The *Federal Cybersecurity Enhancement Act of 2015* also requires agencies to apply these capabilities to "all information traveling between an agency information system and any information system other than an agency information system." *Id.* § 151, note. Notably, these statutory provisions have flexibility regarding the technological means through which DHS offers these intrusion detection and prevention capabilities and is not tied to the current NCPS implementation. Indeed, the Homeland Security Act encourages development of these capabilities by requiring DHS to "regularly assess through operational test and evaluation in real world or simulated environments available advanced protective technologies to improve detection and prevention capabilities, including commercial and noncommercial technologies and detection technologies beyond signature-based detection, and acquire, test, and deploy such technologies when appropriate." *Id.* § 151(c)(4).

overlooked areas of the IT ecosystem, which are more vulnerable and at higher risk of attack or exploit.

Additionally, when individual agencies issue agency-specific IT contracts, they reinforce the current emphasis on boundary protections and limit opportunities for applying economies of scale in provisioning common network and security services for the Federal Government. Small agencies, especially, often lack staff resources and technical expertise to securely manage existing networks, migrate to new computing models, and navigate security acquisition processes. Enabling a new approach to modernization and consolidation of networks requires a strategy that addresses each of these challenges with associated recommendations for legal, policy, resource allocation, acquisition, and workforce interventions, as detailed further below.

Future State & Objectives

The future of Federal IT is one in which agencies move further toward a risk-based approach to securing their systems that places appropriate emphasis on data-level protections and that fully leverages modern virtualized technologies. This renewed focus on data-level protections for managing risk must be accepted and driven by agency leadership, mission owners, IT practitioners, and oversight bodies. Specific recommendations that will bridge to this future state are detailed in the next section, titled "Implementation Plan." The following broad objectives will drive momentum toward the future state of IT:

Reduce the Federal attack surface through enhanced application and data-level protections.

Rather than treating Federal networks as trusted entities to be defended at the perimeter, agencies should shift their focus to placing protections closer to data, specifically through improved management and authentication of devices and user access, as well as through encryption of data – both at rest and in transit. This approach curtails an attacker's likelihood of gaining access to valuable data solely by accessing the network, and it has the potential to better block and isolate malicious activity. As agencies prioritize their modernization efforts, they should implement the capabilities that underpin this model to their high value assets first.

Improve visibility beyond the network level.

Agencies will gain greater visibility and resilience against more sophisticated attacks, including insider threats that may have access to agency-owned networks by enhancing protections closer to the data. Expanding visibility beyond the network level – for instance, through collecting security logs at the application level or establishing a vulnerability disclosure policy and placing systems or applications under a bug bounty program – provides security teams with other information feeds, which they can use to better understand, process, and triage information security events and possible incidents. This information can provide insight into the gaps in security that agencies are experiencing, which informs the types of investments they should make to defend against modern threats. Maximizing the effectiveness of this approach requires updating tools and models by which staff conduct operational security to detect and prevent intrusions. It also requires risk-proportionate application of security practices and maintenance

of situational awareness, particularly in scenarios in which Federal information resides in an off-premises environment, such as in commercially-provided clouds. Government-wide programs designed to deliver these tools and services must evolve, as must the operational culture by which agencies collect and analyze logs and interact with the security research community.

Ensure that policy, resource allocation, acquisition, and operational approaches to security enable use of new technology without sacrificing reliability or performance.

Information technology policy, resource allocations, acquisition processes, and operational guidance must enable the achievement of security objectives while also allowing agencies to take advantage of newer approaches to technology, such as commercial cloud-based services and mobile devices. Agencies should prioritize the IT resources and technical personnel they need to implement necessary data protections and provide situational awareness in their daily operations, whether information is stored on premises or in a commercial cloud. While some successes have occurred in the Federal Government, many real or perceived impediments remain to accelerating network consolidation and optimization on a Government-wide scale. The recommendations in this report collectively address and seek to remedy impediments to modernizing Federal IT. Addressing these barriers will enable agencies to accelerate toward a new era of modernization without sacrificing security or performance.

Implementation Plan

This section outlines immediate next steps and long-term considerations related to the modernization of Federal networks. The focus areas below accelerate Federal efforts on three core concepts: (1) prioritizing high value assets; (2) adopting security frameworks that better protect systems at the data level; and (3) consolidating and standardizing network acquisitions and management wherever possible.

1. Prioritize the Modernization of High-Risk High Value Assets (HVAs)

The HVA Initiative, which began in 2015, was a seminal step in helping the Federal Government recognize, categorize, and prioritize modernization and security improvements for the primary benefit of its "crown jewel" systems.[10] The implementation plan outlined below goes a step further by recommending specific policy, resource allocation, and other interventions to provide near-term assistance to agencies as they strengthen their ability to protect these assets, which are susceptible to the greatest amount of cybersecurity risk. It leverages the current ATC supported efforts to improve the Authority to Operate (ATO) process, and it corresponds with the direction set forth in Section 1 of EO 13800, which mandates that all agencies perform a risk assessment and identify areas in which additional attention is needed. This is consistent with agency responsibilities under FISMA.

Simply applying the next set of patches to these systems and tacking on additional tools is no longer sufficient; rather, HVAs must be driven toward implementation of modern architectures

[10] OMB Memorandum M-17-09, *Management of Federal High Value Assets*.

that are based on data-level protections. Systems that are most important to the Federal Government, yet are also most vulnerable, should be addressed first.

Next steps to support this recommendation are as follows:

Immediate Action:
It is recommended that the President direct the implementation of the plan outlined below to improve the security of high-risk HVAs by migrating to a modernized architecture and employing security best practices.

Within 30 days of the date of issuance of this final report:
Consistent with relevant portions of the enterprise risk management plan to be developed pursuant to Section 1(c)(iv) of EO 13800, Commerce's National Institute of Standards and Technology (NIST) will provide OMB with a plan to promote a risk management culture that focuses agency effort on the operational performance and compliance of their most valuable systems, while simultaneously allowing for the deployment of low-impact systems in a less burdensome and less costly manner. This plan will include a process and timeline for revising Federal Information Processing Standard (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. The plan should also include proposed updates to any other relevant NIST Special Publications (SPs) to enable and support improvements in agency risk management processes that lead to the appropriate selection, implementation, and continuous monitoring of controls and capabilities commensurate with the risk to information, systems, agency missions, and individuals. These updates should include the use of the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), and, where appropriate, incorporate lessons from other control and compliance frameworks, such as ISO, SOC 2 Compliance Audits, and Payment Card Industry. These updates should review the security requirements for these other frameworks and system approval processes used, and assess the use of overlays of these frameworks as a viable approach and intended for inclusion into the proposed updates of the relevant Special Publications.

Within 60 days of the date of issuance of this final report:
Consistent with Section 1(c)(iv)(B) of EO 13800, DHS, in consultation with OMB, will provide a report which identifies common areas of weakness in Government HVAs. The report will include recommendations for addressing these risks Government-wide, informed by agency risk assessments, as well as past and current Risk Vulnerability Assessments (RVAs), and Security Architecture Reviews (SARs) DHS has performed on various agency HVAs.

NIST will provide OMB with a plan to improve cryptographic agility in the Federal enterprise. This plan will include a process and timeline for revising FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, as well as plans for future cryptographic transitions. The plan will describe how the Federal Government can maintain strong standards for the cryptographic hardware and software modules it uses, while ensuring that associated processes help the Federal Government make rapid use of new cryptographic primitives and advances.

Within 90 days of the date of issuance of this final report:
Pursuant to its statutory authorities and in execution thereof, OMB will update the annual FISMA metrics as well as the Cybersecurity Cross-Agency Priority (CAP) Goal metrics to focus on those critical capabilities that are most commonly lacking among agencies. OMB will focus oversight efforts, including CyberStat Reviews and President's Management Council (PMC) Cybersecurity Assessments, on driving progress on these capabilities, with a specific focus on HVAs.

DHS, in consultation with OMB, will work with agencies, including by issuing direction when appropriate, to support mitigation actions to address common areas of risk identified in the Report to the President on Risk Management in accordance with their authorities.

Within 120 days of the date of issuance of this final report:
Consistent with Section 1(c)(iv)(B) of EO 13800 and in execution of their independent statutory authorities, OMB and DHS, will develop a strategy for an approach that clearly describes the lines of authority and operating procedures necessary. This strategy will optimally realign resources across agencies to reduce the risk to HVAs across the Federal enterprise and respond to cybersecurity incidents for those assets. These efforts should align with the recommendations identified in the plan to adequately protect the executive branch enterprise in response to agency risk management reports, per Section (1)(c)(iv) of EO 13800.

Within 150 days of the date of issuance of this final report:
CIOs, Chief Information Security Officers (CISOs), and SAOPs will review their latest submission of HVAs to DHS and OMB, and will make any necessary changes to reflect the latest information on system prioritization in tandem with the assessments made under their risk assessments as part of Section 1 of Executive Order 13800.

Within 180 days of the date of issuance of this final report:

DHS, OMB, and the National Security Council (NSC) will review HVA lists submitted to DHS by Federal agencies and will produce a prioritized list of systems for Government-wide intervention. Six HVAs will be selected to receive centralized interventions in staffing and technical support, and the broader, prioritized list will be vetted by the PMC. Additionally, agencies will work with OMB to reallocate their IT resources appropriately in order to align and adequately resource the modernization of HVAs.

Consistent with the current HVA Program that is administered by DHS and overseen by OMB, any agency that has an HVA that has been identified as having a major or critical weakness in either a risk assessment, RVA, SAR, or an agency-sponsored review will identify a remediation plan. Where the corrective action for a critical weakness for an HVA can be attributed to obsolete or unsupported technology, or critical deficiencies in the solution architecture, the remediation plan shall include a proposal for accelerating modernization within one year and identification of impediments in policy, resource allocation, workforce, or operations. This plan should maximize use of shared IT services, implement application and data-level protections, and emphasize appropriate use of FedRAMP authorized cloud-based architectures. Specific recommendations for modern security approaches are described in Appendix A. Agencies should prioritize existing financial and human resources

and should identify other systems of concern that may suffer from similar issues, but that are not categorized as HVAs.

Where possible and subject to funding, OMB, through the U.S. Digital Service (USDS), and GSA will support DHS in providing hands-on technical assistance to agencies in bolstering protections for systems identified through this process as having the greatest need for modernization.

Additionally, DHS will work to expand the availability of RVAs and SARs for agency HVAs. OMB will also work with DHS to refocus these assessments to concentrate on hands-on technical engineering interventions, de-emphasizing the review of system documentation and policies. In addition, OMB and DHS will work with GSA to expand the visibility, offerings, and agency use of the Highly Adaptive Cybersecurity Services Special Item Numbers (HACS SINs) on IT Schedule 70.

Within 365 days of the date of issuance of this final report:
Pursuant to its statutory authorities and in execution thereof, OMB will work with DHS, GSA, and other stakeholders to capture standard operating procedures for the protection of HVAs and will develop a playbook that agencies can leverage to expand this approach to other systems in a prioritized, risk-based fashion in accordance with FISMA.

2. Modernize the Trusted Internet Connections (TIC) and National Cybersecurity Protection System (NCPS) to Improve Protections, Remove Barriers, and Enable Commercial Cloud Migration.

The perimeter-based security model employed by Federal agencies today, formalized in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*, focuses on standardizing security at the network boundary by consolidating external access points. Under this model, agencies are required to reduce external connections to a target of 50 and route their traffic through this limited number of secure gateways. These gateways apply common security protections, as well as common intrusion detection, information sharing, and prevention capabilities under DHS's NCPS. NCPS consists of three sensor capabilities, collectively referred to as EINSTEIN, as well as a set of analytic tools used by cyber analysts to find, identify and categorize cyber threat activity.[11]

The NCPS sensor suite is deployed in three iterations: EINSTEIN 1, which captures and analyzes network flow information; EINSTEIN 2, which incorporates intrusion detection technology that scans the content of network communications to identify and alert users to known indications of malicious activity; and EINSTEIN 3-Accelerated (E3A), which detects and blocks malicious activity through domain name systems (DNS) sinkholing and email filtering. The TIC policy, and subsequently the *Federal Cybersecurity Enhancement Act of 2015*, requires agencies to utilize these capabilities, which are currently provided through NCPS, to protect all information traveling between an agency information system and any external information system.[12] This perimeter-based model sought to provide a means to aggregate all Federal Executive Branch

[11] See Footnote 9.

[12] *Federal Cybersecurity Enhancement Act of 2015*, *Consolidated Appropriations Act of 2016* (Pub. L. No. 114-113, 129 Stat. 2242, Division N, Title II, Subtitle B).

traffic so that the Government can apply common methods, such as classified indicators, to protect against information security threats and maintain consistent situational awareness.

This approach of perimeter-based network security has created several challenges for agencies wishing to take advantage of commercial cloud services.[13] DHS recognizes these challenges, and has articulated initial steps toward addressing these specific challenges in Appendix C of this report. DHS will provide recommendations on how the NCPS and Continuous Diagnostics and Mitigation (CDM) programs can be updated to enable a layered security architecture that facilitates transition to modern computing in the commercial cloud.

Next steps to support this recommendation are as follows:

Immediate Action:
It is recommended that the President direct the implementation of the plan outlined below to accelerate secure use of commercial cloud through the modernization of the NCPS Program and TIC capabilities, policies, reference architectures, and associated cloud security authorization baselines. This effort will support the prioritization of security resources from lower-value assets to higher-value assets, enabling agencies to build out data-level protections in furtherance of a layered security architecture, and directly accelerating commercial cloud adoption. This effort will be driven by agency use cases, which will also be used to inform rapid updates to policy. This modernization effort will prioritize work to focus on cloud-ready projects and target agencies struggling to comply with the TIC policy and cloud adoption efforts to provide more immediate relief. The goal is to accelerate migration on three cloud-ready systems within the next year. OMB will codify this plan in an update to TIC policy, to provide agencies clear direction on the path forward. The entire process described below will be overseen directly by the ATC, including weekly status updates to the Director of the ATC regarding progress.

Within 30 days of the date of issuance of this final report:
Pursuant to its statutory authorities and in execution thereof, OMB will submit a data call to agencies requesting submission of both in-progress and pending projects for cloud migration. Agencies should focus submissions on projects that have experienced delays due to constraints in current TIC policy and NCPS program implementation, and should propose a migration plan that highlights needed changes to requisite policies and capabilities to facilitate faster migration.

Within 60 days of the date of issuance of this final report:
The ATC, supported by GSA, will include the FedRAMP project management office (PMO) and the Technology Transformation Service (TTS), DHS, OMB to include USDS, NSC, and other relevant parties will review these submissions and bucket them into three categories:

1. Systems that are sufficiently low risk to migrate to cloud immediately. These systems will be migrated to the cloud, and lessons learned will be captured and used to pilot further changes to existing policy. These systems will also be the focus of additional updates to

[13] DHS Office of the Inspector General. *Implementation Status of EINSTEIN 3 Accelerated.* March 2014. U.S. Government Accountability Office (GAO) Report 16-294, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of its NCPS.* January 2016.

the FedRAMP baselines to explore further tailoring of controls for low-risk systems.[14]

2. Systems that are high-priority cloud migration candidates but present a level of risk significant enough that external assistance is necessary to ensure secure migration. This will represent a small number of "implementation validation case studies" that will receive technical assistance in support of their migrations. Lessons learned from these case studies will be used to inform new approaches to TIC and NCPS policy and operations.

3. Systems that are such high risk that they should not be migrated until further policy direction is given or capability enhancements are made. These systems will be assessed to evaluate whether there are common features or capabilities that could be provided efficiently, effectively, and securely by cloud service providers (CSPs). This analysis will serve as an input to the FedRAMP Joint Authorization Board (JAB) prioritization of high-baseline CSP offerings available to agencies wanting to migrate high-impact data to the cloud.

To codify this approach, OMB will provide a preliminary update to the TIC policy that introduces a 90 day sprint during which projects approved by OMB will pilot proposed changes in TIC requirements. This update will also formalize the approach outlined above and in the subsequent two sections.

Within 90 days of the date of issuance of this final report:

1. For Category 1 of projects above, agencies will be given approval to begin cloud migration by following their proposed migration plans. GSA, DHS, OMB, and NSC will require collection of metrics, which will be used to ensure that the proposed changes to policy do not introduce an unacceptable level of cybersecurity risk. Agency project teams would capture these metrics and lessons learned from these migrations and submit initial findings to GSA, DHS, and OMB. These inputs will inform changes to the TIC policy, Reference Architecture (RA), and NCPS operational model and outcomes and to further tailoring of the FedRAMP baselines. These activities will be undertaken within the understanding that agency heads still own the risk for the system authorizations and control decisions they are making.

2. For category 2 projects above, GSA, DHS, OMB, NSC, USDS, and other relevant parties will kick off a 90-day sprint to validate particular case studies. The exact number of engagements will be driven by staffing considerations from these organizations, but will consist of at minimum three test cases. These test cases will be operational in nature, and will validate a subset of implementation plans for improving the TIC policy, RA, and NCPS operational model and outcomes in commercial cloud.

3. For category 3 projects above, GSA, DHS, and OMB will work with agencies to evaluate whether there are common features or capabilities that could be provided efficiently, effectively, and securely by CSPs. This analysis will serve as an input to the FedRAMP JAB's prioritization of high-baseline CSP offerings available to agencies wanting to migrate high-impact data to the cloud.

[14] This approach was originally piloted by the FedRAMP Tailored baseline, which is designed to increase FedRAMP's flexibility to rapidly authorize and use low-risk applications. FedRAMP Tailored was finalized in September 2017, and can be seen at https://tailored.fedramp.gov/policy/.

Within 180 days of the date of issuance of this final report:
DHS, GSA, and OMB will use the information gathered from the activities listed in the section immediately preceding to inform rapid draft updates to the TIC policy, the associated reference architectures (RA), and any appropriate NCPS operational models to facilitate outcomes in commercial cloud. The updated draft will codify the findings from these case studies, as well as holistically address incentives and barriers for agencies in securely migrating to commercial cloud solutions. Example areas that we plan to look at as part of the case studies may include the following:

- A recommendation as to whether (1) "all information" traveling to and from agency information systems hosted by commercial cloud providers warrants scanning by DHS through NCPS; (2) which NCPS capabilities are most applicable in commercial cloud environments of differing asset value; and (3) what new NCPS capabilities may be required to maximize effectiveness in a commercial cloud environment;
- How the current NCPS model could be adapted to accommodate a larger number of access points per agency, including any number of virtualized access points for agencies who are migrating their services to cloud environments;
- Requirements to enable lifting the constraint of two TIC Access Points per agency with assurance that consistent configuration management is applied, information is shared, and new updates are deployed rapidly;
- How agencies can best incorporate intrusion detection and prevention capabilities into their use of cloud services in a way that ensures adequate visibility to agency operators and helps DHS to protect Federal information. Updates to the capabilities outlined in applicable OMB Memoranda and DHS's TIC RA to revisit the critical capabilities for boundary protection, de-emphasize the prescribed architectural implementation, and focus on capabilities, especially those that serve as compensating controls for commercial cloud environments;
- Which TIC capabilities, if any, are appropriate for traffic associated with systems protecting FISMA-Low data, or any lower impact data as aligned with the tasking for Commerce's proposed revisions to FIPS Publication 199 and 200;
- The impact of allowing traffic associated with systems deployed to commercial cloud to not employ physical TIC protection if those systems meet the appropriate operational security capabilities for cloud described in the updated RA;
- Best practices agencies should follow in implementing protections at other levels beyond the network, including how these practices should be integrated with the agencies' network security program;
- Elimination of the existing TIC-related FISMA metrics and manual TIC Compliance Validation (TCV) process, replacing both with automated metric collection, to the extent possible, with a primary focus on both security and availability measures. This should leverage, to the extent possible, existing capabilities under the CDM program and build on previous research DHS has undertaken to automate TIC compliance using this program; and
- Options for the reallocation, if necessary, of current TIC-related DHS personnel and resources toward helping agencies resolve operational issues in cloud migration.

3. Consolidate Network Acquisitions and Management

The current model of IT acquisition wherein each agency, and often multiple components within a single agency, purchase goods and services independently has contributed to a fractured IT landscape. This creates an inconsistent security posture and fails to maximize the buying power of the Federal Government. To alleviate this problem, the Federal Government is implementing category management principles to consolidate and standardize network and security service acquisitions to take full advantage of economies of scale, reduce burden, and dramatically improve technical development and operations. The Enterprise Infrastructure Service (EIS) contract is the vehicle the Government will use to implement the strategy that achieves these goals.

Currently, GSA is transitioning agencies from the legacy Networx contract, under which agencies purchased $1.79 billion in network and telecommunications services in fiscal year (FY) 2016, to a comprehensive solution-based contract vehicle called Enterprise Infrastructure Solutions (EIS).[15] The purpose of EIS is to address all aspects of agency telecommunications and network infrastructure requirements while also leveraging the bulk purchasing power of the Federal Government. EIS can be leveraged to help address some of the unique challenges faced by small agencies, a community that typically lags behind the large agencies in terms of cybersecurity capabilities.[16] Smaller and non-CFO Act agencies struggle to attract and retain top information security personnel and often lack the expertise to fully manage their information security programs. This impedes the Federal Government's ability to gain a full understanding of the risk to Federal networks. EIS can be leveraged to consolidate acquisition activities and other security services for small agency networks by focusing on the objectives below.

Reduce Wasteful Spending on Duplicative Security Capabilities. Under the current Networx contract, agencies who do not have their own TIC capabilities must procure TIC services by purchasing the full suite of Managed Trusted Internet Protocol Services (MTIPS) services,[17] the bundling of which prohibits agencies from procuring only those tools they need, thereby increasing cost. EIS will allow agencies the flexibility to choose *a la carte* the managed security services tools they need to comply with MTIPS requirements, while still being protected by the intrusion detection and prevention capabilities DHS provides.[18] Though a positive and cost-saving step for many agencies, some small agencies may still struggle to procure TIC-like capabilities in this manner due to the complexity of managing the procurement and integration of multiple vendors; however, when paired with the proposed revisions to the existing TIC policy and RA, agencies will be able to make cost-effective acquisition decisions based on their existing tools and overall risk tolerance.

---

[15] The recently rescinded OMB Memorandum M-08-26, *Transition from FTS 2001 to Networx* stated that all agencies should use Networx to acquire telecommunications connectivity, including the option to purchase Trusted Internet Connections solutions from vendors as a managed service, called Managed Trusted Internet Protocol Services (MTIPS). As of July 2017, an OMB Memorandum mandating a similar use under the EIS contract does not exist.

[16] In this report, "large" agencies refer to the 24 agencies required to appoint agency Chief Financial Officers (CFOs) (i.e., "CFO Act agencies") under the *Chief Financial Officers Act of 1990* (31 U.S.C. §901). All other agencies aside from these 24 are referred to as "small" agencies.

[17] MTIPS providers supply small agencies with a vendor-managed solution that ensures compliance with OMB's Trusted Internet Connection policy.

[18] Pursuant to 6 U.S.C. § 151.

Decrease Risk by Improving Situational Awareness of Managed External Network Connections to the Internet. Approximately 40 of the 102 small agencies supported by the Networx contract currently receive MTIPS services. The result of this gap in MTIPS capabilities is a lack of shared situational awareness regarding the network traffic traversing Federal network boundaries. This lack of awareness makes it difficult to conduct enhanced monitoring of network traffic and ultimately makes it harder to perform incident response activities. Increasing this visibility is critical to the defense of the .gov environment, and the additional flexibilities noted above will enable the remaining agencies to provide the requisite information.

Next steps to support the objectives outlined above are as follows:

Immediate Action:
It is recommended that the President direct implementation of the plan outlined below. This plan will leverage the consolidated buying power of the Federal Government to procure more cost effective and secure network services.

Within 60 days of the date of issuance of this final report:
DHS to provide GSA and agencies with baseline configuration guidance for Managed Security Services (MSS) capabilities offered under EIS in order to maximize the return on investment for the security capabilities procured by agencies and to ensure compliance with current TIC policy.

Within 90 days of the date of issuance of this final report:
GSA, in coordination with DHS, shall develop a comprehensive acquisition strategy that provides a feasibility assessment and roadmap to accomplish the following tasks:

- Provide a path for all small agencies to more easily and cost effectively utilize EIS services. This strategy should ensure the Federal Government is maximizing its buying power when competing contracts under EIS;
- Review current security capabilities currently offered under MTIPS, as defined by the TIC RA, to ensure the capabilities provide adequate security within the current threat environment, and determine if any security capabilities need to be added or removed from the existing MTIPS baseline. This should include an examination, including cost analysis, of the feasibility of providing a service consisting only of traffic aggregation in order to decrease the cost burden on small agencies;
- Identify additional areas of opportunity outside of EIS, such as bug bounty platforms, to consolidate acquisition of cybersecurity services and products; and
- Determine the feasibility of establishing a centralized acquisition support function within GSA that is capable of performing cybersecurity-related contract management activities for small agencies.

Other High-Level Actions:

Increase Economies of Scale through Consolidation of Contracts for Small Agencies. Currently, 102 Federal small agencies are supported by the legacy Networx contract, each on separate task orders. GSA will support these small agencies in the transition to EIS by consolidating requirements for small agencies and is considering the best approach to leverage a limited number of task orders to purchase the majority of

services these agencies need. Through the consolidation of common requirements across small agencies, GSA can leverage one or a small number of task orders under EIS to purchase the majority of services needed for all small agencies, with an option to provide additional specific language focused on agency-specific requirements, in order to realize economies of scale.

Improve Acquisitions Support for Small Agencies to Maximize the Use of MTIPS and other Cybersecurity Services. For small agencies, there are often barriers to acquiring and maximizing the benefits of MTIPS. In addition to high costs, many small agencies lack the appropriate expertise to draft effective task orders and the resources to manage their MTIPS contract and hold vendors accountable for accomplishing the work specified in Service Level Agreements (SLAs). As such, GSA will provide guidance to small agencies on how best to leverage its cross-agency acquisition in order to optimize their IT investments and management throughout the procurement process. GSA will also provide a menu of products and services to meet small agency IT needs, leveraging GSA's buying power and unique position in the marketplace to transfer cost savings to small agencies.

Shared Services to Enable Future Network Architectures

Summary of Efforts to Date

Category Management and Shared Services are both industry leading practices that help the Federal Government deliver common functions in a more effective and efficient way. Category Management allows the Government to buy more like a single enterprise by purchasing commodities and common services consistently and with minimal variation to leverage the Government's buying power. Government-wide Category Managers identify "Best in Class" (BIC) solutions, which are contracting and acquisition designations used to denote contracts that meet rigorous category management criteria as defined by OMB. These designated BICs allow acquisition experts to take advantage of pre-vetted, Government-wide contract solutions. As stated earlier, Shared Services is the provision of consolidated capabilities or functions (services and/or IT systems) that are common across multiple agencies. Shared information technology relieves customer agencies of managing upgrade cycles, maintenance, and acquisition overhead associated with supporting duplicative mission support technologies.

Shared Services intersects with Information Technology Category Management in that common solutions developed under Category Management should be leveraged by all agencies, including organizations providing shared services. Providers assume the responsibility for customers of managing the contracts/orders, ensuring scalability and efficiency of services, holding vendors accountable for meeting performance metrics, and delivering continuous improvement of business process.

Shared services has a long history in the Federal Government and gained momentum with the establishment of functional lines of business with the *E-Government Act of 2002*. Building upon this progress and leveraging best practices from the private sector, in October 2015, OMB announced the formation of the Unified Shared Services Management (USSM) office within GSA to enable the delivery of high-quality, high-value shared services that improve performance and efficiency throughout the Federal Government. USSM's mission is to transform the way Government does business internally to improve the way the Government serves the American public.

While there has long been interest in shared services for general IT needs, a perilous threat environment has resulted in a need for cybersecurity shared services as well as commercially-provided commodity IT, such as email, and the cloud. Not only would the widespread use and deployment of shared services in information security provide cost savings, they would also provide a more consistent level of security across the Federal enterprise.

Current State

Addressing security challenges is critical if the Federal Government expects to achieve strong security outcomes; however, the current model of distributed Federal IT makes tackling complex resource-intensive problems in a consistent manner challenging. Today, each agency must independently identify possible vendors, evaluate the security of the vendors, issue an

ATO, integrate the solution into their own independent bespoke IT infrastructure, and allocate resources to monitor and operate that infrastructure on an ongoing basis. The combination of these factors does not achieve consistent, high-quality security outcomes.

The Federal Government is the world's largest buyer and there is a critical need to change the way the Federal Government buys common information technology products and services. Transitioning to consolidated network architectures and shared services requires consideration of how these products or services will be acquired. Current challenges associated with use of commercial acquisition practices limit the Federal Government's ability to achieve its modernization goals.

Significant contract duplication means that agencies award multiple contracts for similar goods and services, often leading to hundreds, if not thousands, of contracts for the same requirement with the same vendors. Additionally, there are huge price variances for the exact same item, sometimes as much as 300 - 400 percent. Agencies work highly autonomously, with only occasional collaboration across organizations and little sharing of information, standards, and best practices. This degree of fragmentation, lack of common standards, and lack of coordination drives costly redundancies and inefficiencies in procurement actions, contracting vehicles, and customization of common information technology solutions.

The existing federated and distributed approach to IT is no longer sustainable in an increasingly mobile, cloud-based, and complex digital world. Building or internally operating such security programs requires specialized cybersecurity talent and knowledge, access to a broad range of data sources to manage the latest threats, and sophisticated and costly emulation and static analysis technology. This is an immense undertaking for large departments, but even more so for smaller and non-CFO Act agencies who often struggle with basic security functions, such as vulnerability mitigation, due to resource limitations. Programs like CDM are taking steps toward deploying common tools across all agencies and integrating large and small agencies into a shared cybersecurity understanding; however, many of these programs, including CDM, have been mired by delays and have not yet yielded their full promise.

Future State & Objectives

In order to reduce cost, improve operational efficiencies and cybersecurity, the Federal Government must shift toward a consolidated IT model. This includes adopting shared services for non-mission specific functions, as well as BIC contracts, commodity IT, such as email, and other collaboration productivity, and security tools. This approach will help the Federal Government rapidly deploy new capabilities that will enhance agencies' abilities to perform their missions and secure their networks. The Federal Government must embrace the broader use of cloud services while working to develop cloud products that meet Federal cybersecurity standards. With the proper type of cloud offering designed with an appropriate focus on security, the increased use and consolidation of IT services in multi-tenant cloud services can provide the visibility and control necessary to deploy data-level protections and automated cybersecurity outlined earlier in this report. Agencies must leverage shared services and embrace commercial technologies such as Software as a Service (SaaS) where possible, building new capabilities only when shared services and commercial technologies cannot meet mission need.

The NIST Definition of Cloud Computing (SP 800-145)[19] establishes the essential characteristics and service model definition for cloud-based SaaS, which also serves as the definition for this Report and its implementation. Transitioning to a consumption-based service, as opposed to traditional approaches of purchasing on-premise licenses, will enable the Government to stop building systems that are expensive to maintain and modernize. Among other benefits, the Government will only pay for what it uses, better leverage its buying power, achieve the benefits of continuous modernization, and gain economies of scale from standardization.

As Federal agencies increase their investment in commercial cloud services, promoting vendor interoperability and avoidance of "vendor lock-in" will continue to be important priorities. Where feasible and appropriate, the use of tools and platforms that can be used portably across multiple underlying cloud service providers is encouraged. Agencies of any significant size, such as CFO Act agencies, are generally expected to authorize and make use of multiple independent cloud environments. At the same time, agencies are encouraged to make use of the best and most cutting-edge services that cloud service providers have available. This can include services that may be specific to individual providers' and which are optimized for their strengths.

In general, agencies should avoid unhealthy levels of dependence on specific vendors, while taking advantage of the best technologies the commercial market has to offer.

In order to achieve the desired future state, the Government must address the current impediments in policy, resource allocation, Government-wide business standards, and disparate agency interpretations of statutes and guidance, in addition to other considerations that are obstacles to agencies' adoption of shared and cloud services. Such obstacles include statutory and regulatory requirements that prevent the use of accepted commercial best acquisition practices. Changes and modifications to the existing acquisition requirements could be implemented to achieve efficiencies while maintaining the core tenet of fairness. Rather than relying on often outdated and agency-specific systems, the Government should speak with one voice to providers to obtain systems and services that offer world-class levels of functionality that meets the Government-wide business standards, achieve cost-effectiveness through economies of scale, and are secure.

Implementation Plan

Both the short- and long-term steps outlined in this section will result in greater innovation across the Federal enterprise, decrease costs, and dramatically improve services provided to both agencies and citizens. These interventions will allow agencies, and particularly smaller agencies, to more easily acquire and adopt commodity cloud infrastructure products, while leveraging the Federal Government's buying power to produce economies of scale. Additionally, these efforts will augment existing agency-specific technology to improve both visibility and security. This implementation plan focuses on three key areas viewed as pivotal for accelerating the move to shared services: (1) enabling the use of commercial cloud services and infrastructure; (2) accelerating adoption of cloud email and collaboration tools; and (3) providing additional and improving existing shared services.

[19] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*.

1. Enable the Use of Commercial Cloud Services and Infrastructure

Major commercial cloud infrastructure providers offer excellent levels of functionality, cost effectiveness, and security because of their ability to aggregate demand across a broad range of customers. There are a wide range of ways each of the models outlined below can drive cloud adoption by Government customers; however, it is generally helpful to think about the options as one default approach and a second option when security requirements require it.

- **"Bring the Government to the Cloud."** This approach is the recommended default approach the Government should utilize and is characterized by multitenant commercially owned infrastructure (e.g., building servers, networks, applications) that is shared with other non-Government customers, but in which Government data is protected through security technologies and encryption.
- **"Bring the Cloud to the Government."** This approach is characterized by multitenant Government-owned and -operated infrastructure (e.g., buildings, servers, networks, applications) or commercially owned and operated infrastructure isolated and dedicated for Government use.

In order to ensure a smooth adoption of cloud technologies across the Government, it is important to understand the various models that are available for utilizing cloud services. The following two options describe the main approaches in which the Government has adopted cloud services and how these models could be adjusted moving forward.

Bring Government to the Cloud: Vendor-owned And operated servers and applications — Software as a Service (SaaS)

This is the ubiquitous public cloud model used by the vast majority of private sector cloud providers, and is in use by some Federal agencies today. Among other uses, this model may be appropriate for modern cloud-hosted email, productivity, and collaboration tools and mission support services.

Many agencies have already fully embraced vendor-operated, cloud-based collaboration and productively tools, and, depending on the agency, may have several such tools based on commercial SaaS in use today in their environment. It is important for the rest of Government to migrate from legacy offerings to take advantage of the increased productivity and innovation that these cloud based services offer.

Bring Government to the Cloud: Vendor-owned and operated servers and Government-operated applications with networks that utilize a secure connection — Infrastructure as a Service

Some service needs can only be met by developing custom software, or by buying software not available as a service. With this model, a cloud vendor owns and operates servers in a private sector data center, but connected through a secure connection. Secure connections could include HTTPS, TLS, peering, etc. This provides an infrastructure upon which agencies deploy applications that they create or acquire. This model can be utilized for secure, critical applications that are only available to Government users on a virtual private network (VPN) or other network-level isolation.

Because Infrastructure as a Service gives customers control over many low-level details, it can entirely replace the need for a traditional on premise data center. Agencies can often move existing services from legacy on premise data centers to cloud infrastructure with some software modifications.

These applications can be public services used by the general public or private internal services used by agency employees. In either case, agencies may consider cloud infrastructure as a service to be an extension of their existing private enterprise network, or they may treat it as a separate, isolated network. Regardless, users access the service through secure connections, which could include HTTPS, TLS, VPN, or a dedicated line.

Infrastructure as a service excels at providing a platform for creating and deploying the digital services that are core to an agency's mission. These models are already in use by agencies in a wide range of use cases including benefits processing for veterans, immigration, and healthcare, as well as data processing and software testing in the Department of Defense community.

Bring the Cloud to Government: Government-owned data center buildings with vendor-owned and operated services

For certain applications where using the Internet is not a viable option, commercial providers can operate infrastructure in Government-owned facilities. This is attractive for classified systems that cannot be connected to the public Internet. For example, the intelligence community was the original adopter of a model in which vendor-owned and operated services were based out of Government-owned data center buildings. An example of this approach is the Intelligence Community Information Technology Enterprise (IC ITE) Commercial Cloud Services.

This model is much more expensive than fully commercial cloud services, and cannot keep pace with the innovation of public cloud solutions. As such, it is only appropriate where the Government absolutely must retain physical control over the infrastructure.

It is important to be wary of on premise solutions that are sold with cloud terminology that do not actually meet the NIST Essential Characteristics of Cloud Computing.[20] Often, products that claim to offer private cloud infrastructure fail to deliver on these promises, missing key aspects such as rapid elasticity, on-demand self-service, or resource pooling.

Bring the Cloud to Government: Vendor-owned and operated data centers with servers dedicated for Government use

Many cloud service providers offer Government-dedicated versions of their services, where the provider builds segregated space for Government use so that agency customers only share logical space (possibly including servers, buildings, networks, personnel) with other Government customers. This allows a provider to more easily meet Government-specific compliance requirements for securing sensitive data.

[20] NIST Special Publication 800-145, *The NIST Definition of Cloud Computing*.

This model provides a middle ground between public shared cloud infrastructure and costly on premise infrastructure. It is used by many agencies today to house applications where legal, compliance, or security reasons preclude the use of shared servers.

This model, which is already in use, could be particularly useful and appropriate for hosting Government websites and services for infrastructure that may have sensitivities for which public servers would not be appropriate.

Recommendations:

Cloud is not a one-size-fits-all solution, and offers a multitude of options for agencies based on their needs and preferences. While it is important to ensure flexibility across the Federal Government, there are a few models that can cover the majority of Federal use cases. As such, the Government should invest in two to three cloud models to support the differing security and risk-tolerance postures of agencies and leverage shared services. Further, agencies should work cooperatively and collaboratively to build trust within their own enterprise and between agencies so that Federal programs and system owners can make maximum use of authorization packages, compliance materials, and any other documents or process that promotes reuse and appropriate risk acceptance when deciding to bring new systems online or evaluate legacy systems for migration or decommissioning.

In particular, the Government should expand its use of the "Bring the Government to the Cloud" models, as these best balance the benefits of cloud computing—including improved performance and cost-savings—with outsourced security and control. While the impending revisions to the TIC policy and guidance will affect some of the eventual business decisions surrounding cloud options, agencies should begin working to determine how best to use the models outlined above. Next steps to support the above recommendations are as follows:

Within 30 days of the date of issuance of this final report:
Pursuant to its statutory authorities and in execution thereof, OMB will conduct a data call requesting that agencies identify systems that may be ready for cloud migration and can be migrated securely but have not yet migrated due to perceived or encountered difficulties. At the conclusion of this data call, OMB and GSA will review the impediments to moving to the cloud outlined by agencies and will prioritize an infusion of technical talent, capital, and updated security policy (developed iteratively to solve agency-specific issues) as needed to enable prioritized cloud migrations. This task is described in more detail in the following section.

Within 90 days of the date of issuance of this final report:
GSA will work with volunteer agencies to pilot new initiatives to improve the speed, reliability, reusability, and risk acceptance transparency for cloud-based SaaS and shared services ATOs. Initial pilots will test new authorities and tools for authorization processes as automation of the new NIST Risk Management Framework for select information systems, implementing the new FedRAMP Tailored baseline for low-impact SaaS products, and leveraging Authorizations to Use for shared services based on commercial cloud offerings.

Based on the combined efforts, including lessons learned and best practices for extending these pilot activities to a Federal civilian-wide scale, GSA will work with OMB to develop any

necessary plans or policy for promoting these initiatives and any other innovative FedRAMP, shared services, or agency-specific efforts across the Federal enterprise.

Within 120 days of the date of issuance of this final report:
Pursuant to its statutory authorities and in execution thereof, OMB, in coordination with DHS, GSA, and its Federal partners, will update the Federal Cloud Computing Strategy ("Cloud-First").[21] This strategy will provide additional guidance to agencies on the most impactful use cases for cloud adoption and how best to conduct appropriate operational security in cloud environments.

Additionally, OMB will conduct a thorough review of all relevant policies pertaining to IT modernization, cloud migration, infrastructure consolidation, and shared services, among others, and will initiate revisions, rescissions, or other rapid policy updates that may improve the ability of agencies to modernize effectively, securely, and efficiently. If necessary, OMB will issue further guidance that will augment and enhance existing Federal technology and information security policy.

OMB, working with the Federal Acquisition Regulation (FAR) Council, GSA, and DHS will develop clauses that define consistent requirements for security, privacy, and access to data for use in cloud contracts. These clauses will ensure uniformity in contract language and provide rigor to standard Government terms, which would be particularly valuable to agencies lacking relevant technical, legal, or acquisitions expertise to craft, out of whole cloth, such language in their cloud procurements.

Within 180 days of the date of issuance of this final report:
OMB, working with the Federal Acquisition Regulatory Council (FAR Council) and DHS will develop clauses that define consistent requirements for security, privacy, and access to data for use in cloud contracts. These clauses will ensure uniformity in contract language and clear direction in standard Government terms, which would be particularly valuable to agencies lacking relevant technical, legal, or acquisitions expertise to craft, out of whole cloth, such language in their cloud procurements.

These actions are in addition to OMB's ongoing work with the FAR Council to reduce regulatory burden on federal IT contractors pursuant to E.O. 13771, as well as efforts with members of the Chief Acquisition Officers Council to identify statutory or administrative changes to align federal procurement practices with successful commercial buying strategies and collaboration with agency Acquisition Innovation Advocates to apply modernized processes to improve the acquisition system's ability to support the goals of this report.

2. Accelerate Adoption of Cloud Email and Collaboration Tools

Accelerated adoption of tools like cloud email and collaboration applications is an essential element to achieving timely collaboration capability across the Government. Deploying these tools for the Federal Government sooner rather than later minimizes exposure of one the most prominent cyberattack methods in modern society. Targeted, email-based spear phishing

[21] "25 Point Implementation Plan to Reform Federal Information Technology Management." December 2010.

attacks using malicious attachments and links are the primary attack vector for compromising individuals and organizations.

Accelerated rollout of cloud email and collaboration is urgent given the number of duplicative legacy systems and their associated cybersecurity risks. In addition, even within cloud-based email, there still exists price variance. Agencies generally negotiate as individual organizations - thus limiting the potential economy of scale that could have been achieved negotiating through the Government Enterprise. Buying power through Government-wide price negotiations will achieve efficiencies of cost savings and therefore benefit American taxpayers.

In order to support agencies in moving away from their own email servers and solutions, a set of secure, easy-to-maintain, and cost-effective solutions must be available. Industry is well positioned to provide effective security controls, especially when paired with NCPS capabilities and to enable agencies to leverage improved mobile, tablet, and productivity operating environments. There are currently only two hosted solutions deployed in the Federal Government, though additional competitors could emerge. Regardless, a requirement to make better use of cloud-based email and collaboration services increases the Government's leverage in obtaining farther reaching innovative solutions and better pricing.

While the benefits are worthwhile, ranging from cost savings to improved security, the migration itself to cloud-based tools can be costly and burdensome, particularly for smaller agencies. In order to support agencies in their migration, a set of secure, easy-to-maintain, and cost-effective solutions must be made available.

The Government must pursue new acquisition strategies to obtain cloud email and collaboration tools and services. In furtherance of this objective, pilots such as the example outlined in Appendix D may be executed to decrease the administrative acquisition burden, specifically for smaller agencies who cannot leverage large volume discounts or who have acquisition workforce constraints. Additional pilots may include the ability to purchase cloud services on a consumption basis and coordinated purchasing to obtain tiered-based pricing.

One of the fundamental advantages the Government has in seeking products and services is that its size should allow it to leverage competing market forces to drive Government-wide volume pricing and increase the overall speed of migration. The goal would be to incentivize providers through tiered pricing, business strategies, and service level agreements that would produce insight and transparency into any agreement made to obtain cloud email and collaboration tools by the Government.

This would mark a significant departure from existing acquisition marketplaces where existing models are laborious for both Government and industry and fail to truly capture and make transparent items such as volume spending as an aggregated value. In addition, the current process does not always offer sufficient transparency, allowing some agencies to pay less than others. Often, it is the small agencies, who can least afford higher prices, that are penalized.

Next steps to support the above recommendations are as follows:

Within 30 days of the date of issuance of this final report:
OMB will conduct a data call to agencies regarding their current email contracts, prices, and number of mailboxes. It is imperative that the Government obtain an accurate measurement

of the market size of agencies who have not yet migrated to cloud email. While there are clear data on the current need among CFO Act agencies, there is currently no definitive data regarding the adoption of cloud-based email solutions at small and independent agencies. Understanding the full size of the marketplace will enable the Government to maximize its leverage in negotiations with cloud collaboration vendors.

OMB will convene a task force of agencies to finalize a standard set of requirements for cloud email, including both low and moderate security postures for email and cloud collaboration. These requirements, which will build upon previously completed work, will be circulated to all agencies for comment and serve as the basis for acquisition.

Within 60 days of the date of issuance of this final report:
OMB will establish a comprehensive strategy for driving the accelerated migration of agency email and collaboration tools to the cloud for departments and agencies who have still not adopted cloud-based email. This strategy should emphasize achieving both cost savings and improved security.

Within 75 days of the date of issuance of this final report:
OMB will issue updated identity policy guidance for public comment that will reduce agency burden and recommend identity service areas suitable for shared services. GSA will provide a business case to the Federal CIO on the consolidation of existing identity services to improve usability and drive secure access and interoperability. This action will enable secure access and collaboration as a service in a way that improves existing agency-specific implementations, which often have various levels of security and do not include interoperability.

Within 90 days of the date of issuance of this final report:
OMB will assemble an Acquisition Tiger Team (ATT), which will be charged with drafting and disseminating a "quick start" acquisition package that can help agencies facilitate rapid license and migration service acquisitions. This will make it possible for agencies to award licenses and services that may presently have difficulty doing so. The "quick start" package would include market research, acquisition plans, templates for requesting quotes, identified sources of supply, and Independent Government Cost Estimate calculation templates (based on already completed acquisitions).

The ATT, working through the appropriate executive agent, will send out Requests for Information (RFIs) or conduct other market research activities to find qualified small business and socio-economic concerns to leverage set aside programs and other authorities to streamline the migration acquisitions to the greatest extent possible. For example, using the 8(a) Digital Service Initiative or vehicles that have resulted from Category Management efforts in this space.[22]

Within 180 days of the date of issuance of this final report:
The Government should consider incentives for early adoption (migration in the first year following the formalization of the effort), including individualized assistance tailored to a given agency's needs. To assist in such an effort, OMB will create acquisition/migration cadres, consisting of information technology and acquisition specialists that will be sent to

[22] TechFAR Hub, *8(a) Program Digital Service Initiative*.

early adopter agencies to help with license and migration acquisitions-related challenges. Initially, these cadres would draw from agencies that have already completed their migrations, such as the Department of the Justice (DOJ) and acquisition experts from the Digital IT Acquisition Professional Training (DITAP) alumni network.

Within 240 days of the date of issuance of this final report:
OMB, with support from GSA, will pilot new acquisition tactics for cloud email and collaboration licenses including but not limited to those discussed above and outlined in Appendix D.

Other High-Level Actions:
Approved FISMA-Moderate cloud-based collaboration tools currently exist. GSA will continue to work with existing cloud email and collaboration providers, and will prioritize approval of a FISMA-High offering. At the same time, process improvements will continue iteratively to enable agencies to accelerate adoption of cloud services.

Within the Federal Government, having a qualified and agile acquisition workforce is paramount to ensure the Federal Government acquires optimal solutions to achieve successful acquisition outcomes. Providing specialized training and career development opportunities for the acquisition workforce is a critical component for ensuring tax payer dollars are effectively managed and obligated to achieve the requirements addressed in the Federal IT Modernization Report. Providing training and career development opportunities is a priority for cybersecurity adoption, cloud email, and cloud adoption. The Federal Acquisition Certification in Contracting (FAC-C) core plus specialization in digital services is under review and is a component of the DITAP development program. The DITAP program focuses on providing contracting professionals with training and experiential learning opportunities to gain the expertise necessary to better understand the market conditions and drivers, effectively manage risks to successfully plan, and negotiate and acquire digital supplies and services. Moreover, completion of the DITAP development program empowers the graduates to serve as change agents and expert business advisors to members of the integrated acquisition team (program managers, legal, finance, contracting officer's representative and other stakeholders). Having a Government-wide, holistic and integrated training and career development approach is vital to deliver results to the American People and build a stronger more capable Federal Government.

3. Improve Existing and Provide Additional Security Shared Services

As cyberattacks have become more sophisticated, frequent, and easier for adversaries to execute, cybersecurity has continued to escalate as a primary responsibility for all individual agencies and for the Federal Government as a whole. Addressing cybersecurity threats holistically necessitates both a further consolidation of the Federal Government's IT footprint as well as an expansion of shared, centralized services to better leverage Federal buying power, standardize security capabilities, improve the time it takes to detect and respond to incidents, and realize economies of scale from aggregating data.

Continuous Diagnostics and Mitigation (CDM)

DHS established the CDM Program in 2013 to provide Federal civilian agencies with automated continuous monitoring tools to detect vulnerabilities and potentially malicious network activity in near real-time.[23, 24] CDM Phase 1, which is currently being deployed, is designed to determine "what is on the network" by providing agencies with capabilities to identify and remediate vulnerabilities and ensure secure hardware and software configurations on their networks. CDM Phase 2 will focus on "who is on the network" and provide capabilities to detect and manage privileged user access and ensure that only authorized, credentialed users have access to information on the network. CDM Phase 3 will report "what is happening on the network" and provide capabilities to identify and assess anomalies that may indicate a cybersecurity compromise and to implement ongoing assessment and authorization. CDM Phase 4 will focus on expanding data protections for Government information. All CDM capabilities will feed information to both an agency- and Federal-level dashboard, enabling Government-wide visibility into the current state of Federal information security.

Up to this point, CDM has not sought to address cloud-hosted systems and has instead focused on helping agencies secure their on premise networks. While this does introduce some limitations, the program has nonetheless elevated the baseline of cybersecurity across the Government. Over the identified phases, the program will deliver capabilities through various mechanisms, including an "as-a-service model," to ensure that additional capabilities can be provided in a more centralized and standard way.

A challenge in implementing CDM capabilities in a more cloud-friendly architecture is that security teams and security operations centers may not necessarily have the expertise available to defend the updated architecture. To support agency cybersecurity efforts, the Federal Government is working to develop this expertise and provide it across agencies through CDM. Currently, all CFO Act agencies (except the Department of Defense) participate in CDM, as do 44 of the non-CFO Act agencies in the Federal enterprise. CDM will continue to grow and provide sophisticated tools and services to current agencies, while working to onboard the other small agencies not currently served by the program.

This is imperative for enabling the Federal Government to increase security throughout the Federal enterprise. Further targeted actions by DHS's CDM Program Office and agencies can help expedite the modernization and adoption of CDM to identify, detect, and respond to threats in the Federal Government's increasing move to cloud environments and mobile devices.

Within 60 days of the date of issuance of this final report:
DHS, in partnership with agencies and GSA, will complete the acquisition strategy for new, long-term task orders to offer CDM lifecycle support to agencies and provide solution development and implementation for Phases 3 and 4 in addition to future work, including cloud security.

Within 125 days of the date of issuance of this final report:

[23] OMB Memorandum M-14-03, *Enhancing the Security of Federal Information and Information Systems*.

[24] Coordination of Federal Information Policy – Information Security (44 U.S.C. § 3553(b)(6)).

DHS will leverage all available departmental resources, to the extent practicable, to obtain an initial ATO for the CDM Group F Platform. If necessary, DHS will request additional support from OMB, GSA, or other entities to ensure an efficient authorization, consistent with the appropriate security posture required of the CDM Program, potential customer agencies, and the authorizing official. Upon completion of the authorization process, DHS will begin onboarding agencies onto CDM to provide continuous monitoring as a service capabilities.

At the end of the 125 days, DHS will update OMB on the current number and status of remaining Memoranda of Agreement it has established with non-CFO Act agencies (above and beyond the current number of 44). DHS will also submit a plan to OMB that details the expectations and timelines for onboarding non-CFO Act agencies to the CDM Group F Platform.

Within 150 days of the date of issuance of this final report:
DHS will complete the data exchanges between the agency- and Federal-level dashboards to provide enterprise-wide situational awareness of an agency's cyber posture.

Within 180 days of the date of issuance of this final report:
DHS, in partnership with the Federal CIO Council, will implement a concept of operations for the Federal dashboard to include procedures to manage cyber risks across the Federal enterprise, and other factors pertinent to the broader Federal CIO community.

Security Operations Center (SOC) as a Service

The Security Operations Center (SOC), which generally provides central visibility into the state of security on an agency's networks, is an essential component of securing the Federal IT enterprise; however, many agencies lack the resources or expertise to establish their own agency-level SOCs. Given the vulnerability this creates, the establishment of a SOC as a service (SOCaaS) capability is essential to ensure appropriate enterprise-wide visibility, incident discovery, and information sharing among Federal agencies. Such a capability would allow agencies currently lacking such capabilities to purchase them from those agencies with sufficient capacity to offer such a service. This could allow for the creation of specialized offerings. For instance, agencies who have demonstrated expertise in defending cloud applications could expand their current SOC capabilities and offer a SOCaaS, focusing specifically on cloud applications. In addition, contracts can be established with commercial providers to provide SOCaaS offerings. Agencies lacking the requisite expertise could leverage these services to accelerate their migration to commercial cloud capabilities.

Over time, agencies offering SOCaaS could provide a full suite of capabilities to agencies that do not want or need to manage their own operations. This would align with the consolidation of existing networks. A more consolidated SOC would have broader visibility, easier communications, and the ability to add tools not available in a more distributed model.

Specifically, SOC as a Service capabilities could:

- Prevent security capabilities from causing latency issues;

- Apply security protections at the application and data levels which are commensurate with the sensitivity of the data;
- Offer capabilities for multiple types of logs or data flows depending on cloud provider technology and contract specifications; and
- Allow visibility across multiple agency cloud systems to be aggregated and managed centrally.

Within 180 days of the date of issuance of this final report:
OMB, DHS, and GSA will identify potential offerings to provide SOC as a Service capabilities to other agencies across the Federal Government. Additionally, GSA, in coordination with OMB and DHS, will lead contracting efforts to also offer commercially available SOC as a Service capabilities to Federal agencies.

Within 210 days of the date of issuance of this final report:
Any agency that plans to offer SOC as a Service capabilities will provide to OMB and DHS a pricing model in alignment with the cloud migration strategy and timeline outlined above. Additionally, OMB will designate a slate of agencies with insufficient SOC capabilities and require them to establish plans for transitioning to SOC as a Service, whether it is Government or private sector provided.

Other High-Level Actions:
DHS will work with SOC as a Service providers, be it a Government or private sector provider, to ensure that NCPS and CDM capabilities and outcomes can be achieved and that the visibility remains aggregated across cloud and on premise security capabilities. Additionally, agencies designated as potential SOC as a Service providers will establish pilots involving agencies designated by OMB as possessing insufficient SOC capabilities.

Conclusions & Summary of Requests for Engagement

Difficulties in agency prioritization of resources in support of IT modernization, ability to procure services quickly, and technical issues have resulted in an unwieldy and out-of-date Federal IT infrastructure incapable of operating with the agility and security that is required of a multibillion-dollar Federal IT enterprise. In order to aggressively modernize IT systems, the Federal Government will need to maximize use of shared services and commercial capabilities. In furtherance of this objective, existing policies and programs will be rapidly and iteratively updated to eliminate barriers to cloud adoption, and agencies will rapidly migrate applicable capabilities to commercial cloud services. Capabilities which will not be hosted in the commercial cloud will be modernized to leverage modern security protections, and agencies will assess risk of existing capabilities to prioritize resources on protecting the most important systems and information. The Federal Government will also accelerate the adoption of cloud email and collaboration tools, improve and strengthen existing shared services, and provide additional security shared services for agencies.

Achieving these goals will require an active shift in the mindset of agency leadership, mission owners, IT practitioners, and oversight bodies. Federal agencies must consolidate their IT investments and place more trust in services and infrastructure operated by others. Such a change in outlook will allow for greater utilization of shared services, consolidated infrastructure, and cloud-based collaboration tools that can deliver improved functionality and drive cost efficiencies to improve Government operations and citizen services.

Appendix A: Data-Level Protections and Modernization of Federal IT

This report envisions a modern Federal IT enterprise that relies on **logical protections** and **automation**, and is focused on **empirical evidence** and **security outcomes**.

Below are some capabilities and approaches Federal agencies are expected to use to improve the agility of their enterprise and the security of their IT systems.

Logical Protections

Agencies should rely principally on logical protections, such as encryption and granular permissions, to protect data. When designing mitigations, networks should be considered untrusted, and system components should be assumed to be potentially compromised.

Encrypting Data in Transit. Encrypting data as it transits from one device or system component to another protects data from modification or interception from an attacker with a network vantage point. Network routes that transit data between information system components, or between information systems and their users, should generally be treated as untrusted, even within agency-operated networks. In general, systems should rely only on protocols that can safely "fail closed" (default to connection failure), under attack scenarios. Examples include Secure Shell (SSH) or Hyper Text Transfer Protocol Secure (HTTPS).

Encrypting Data at Rest. Encrypting data using tools that implement NIST standards and guidelines, when stored, whether in a database or some other persistent storage, is designed to make that data useless to an attacker, should an attacker gain access to that storage system and copy the data. Effective designs for encryption of data at rest should consider how to limit an attacker's options both during and after the attacker maintains control of the information system, such as by requiring the presence of a hardware security module to perform (and rate limit) decryption actions. Like encryption in other areas, encryption at rest generally requires sufficiently strong encryption keys with sufficient randomness in key generation.[25]

Multi-Factor Authentication. The goal of multi-factor authentication is to make remote attacks unattractive, typically by requiring the production of a credential that is connected to a specific user in a physical manner in order to grant the user access to a system. Recent Federal efforts have focused on multi-factor authentication for privileged users, or those with elevated access privileges, but thus far has largely centered on network access rather than system and application-level access.

Least Privilege. The principle of least privilege is intended to prevent the compromise of individual users and information system components to lead to the total compromise of an information system. This principle can be applied both to users and to components of information systems. Privileged users should only be granted privileged access to the system components they need to perform their job, which can require richer permissions models than simply designating "admins." Similarly, system components, such as individual servers and

[25] See NIST SP 800-133, *Recommendation for Cryptographic Key Generation*.

endpoints, should themselves be limited in their ability to connect or exchange information to only the components they need in order to perform their function. Mature privilege management programs may also be able to leverage policy- or attribute-based access controls, wherein sophisticated rules-based policies (which can be dynamically updated and enforced) can support a system that makes privilege escalation more expensive and difficult for an attacker.

Application Whitelisting. The purpose of application whitelisting is to allow only approved applications and application components (libraries, configuration files, etc.) to run on a host according to a well-defined baseline, while preventing all other applications from running by default. When implemented, application whitelisting is an effective security technique that helps stop the execution of malicious malware and other unauthorized software.[26]

Mobile Device Management. Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other devices typically used within Government facilities, such as desktops and laptops. When planning mobile device security policies and controls, agencies should assume that mobile devices will be acquired by malicious parties who will attempt to recover sensitive data either directly from the devices themselves or indirectly by using the devices to access the organization's remote resources. Therefore, a layered mitigation strategy should be used that includes user authentication to the device, protection of data either through encryption or by not storing data on the device, and user training and awareness to reduce the frequency of insecure physical security practices. Additionally, agencies should plan their mobile device security on the assumption that unknown third-party mobile device applications downloadable by users should not be trusted. Risk from these applications can be reduced in several ways, such as prohibiting all installation of third-party applications, implementing whitelisting to allow installation of approved applications only, verifying that applications only receive the necessary permissions on the mobile device, or implementing a secure sandbox/secure container that isolates the organization's data and applications from all other data and applications on the mobile device.[27]

Automation and outcome-oriented security

Agencies should gain confidence in their security posture through empirical evidence and measurable improvement over time. To do this, agencies must take an iterative approach to security, and have the agility to change their practices to adapt to the threats they and other agencies observe. Automation is a critical tool to maintain agility in system design and to make the best use of finite human resources.

External Security Testing. Agencies must take a layered approach to penetration testing and system assessments that incorporates as much ongoing external review as possible. At a bare minimum, agencies should establish vulnerability disclosure policies for at least their public-facing services, so that security researchers and other members of the public can report vulnerabilities they discover. Agencies should also identify systems that are appropriate to place under public bug bounty programs, such as those run by the Department of Defense or GSA.[28]

---

[26] See NIST SP 800-167, *Guide to Application Whitelisting*.

[27] See NIST SP 800-124, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*.

[28] United States Digital Service, *July 2017 Report to Congress,* "Hack the Pentagon." July 2017.

Private bounty programs, where researchers may be vetted, monitored, and given credentialed access, can be an additional useful tool for building confidence in a system, and can be run in parallel to, or in advance of, a public program. Bounty programs require vulnerabilities to be fixable in a reasonably rapid time frame, and can be implemented for specific systems, for short periods of time or on an ongoing basis. Agencies have many options for incorporating external security testing of their systems, and should bring as many as feasible to bear on their most important systems.

Avoiding security through obscurity. Internet-wide scanning and discovery is commonplace and effective. Agencies must assume that their publicly accessible systems are trivially publicly discoverable to adversaries, and prioritize the sharing of information about their systems with defenders inside and outside the Federal enterprise. Similarly, agencies should support the use and release of open-source software where it improves agency agility and resilience.

Threat Modeling. Agencies should use threat modeling to understand and drive improvements in the security of their systems. Threat models define what threats a system is designed to mitigate, and what threats the system is not designed to mitigate. This focuses resources in the areas where risk reduction is needed the most, and forms a cornerstone of implementing a risk-based practice of security, as described in the NIST Cybersecurity Framework.

Continuous integration and code review. Agencies should follow a "DevSecOps" model, using automated unit and integration tests to aid the code review process and maintain ongoing confidence in the system. Rather than onerous change control boards, agencies should employ automatic testing and widely visible code review to measure and accelerate the time it takes for code changes to be deployed to production.

Automated Deployments. System deployments should be automated to the greatest extent possible, removing the potential for errors caused by breakdowns in internal processes. To support this, configuration and environmental details that support system deployment should be versioned and managed similarly to the software that comprises the system itself. This practice is necessary to achieve long-term consistency among critical system components, maintain adequate patching, and update velocity.

Immutable Deployments. Production deployments should be automated and designed so that components are not modified in place between deployments. Modification should be technically constrained wherever possible; for example, deployed servers should not allow remote logins. By taking advantage of virtualized infrastructure, new deployments can create brand new instances of deployed system software and supporting components, rather than updating the existing environment in place. This approach allows system owners to design their security architecture and monitoring to treat any in-place modification as a potential attack, and to use more comprehensive technical constraints on modification that remove opportunities for attackers to persist in a deployed environment.

Timely Patching. Unpatched software vulnerabilities remains one of the most significant threats to Federal IT systems. DHS currently scans external-facing agency systems for known unpatched vulnerabilities, and agencies are currently required to patch critical vulnerabilities within 30 days; however, depending on the severity and ease of exploitation, unpatched

vulnerabilities in public-facing systems can lead to compromise in weeks, days, or even hours of public disclosure. Agencies should consider patching agility and responsiveness to be a critical security metric and modernization goal. Automated scanning, consistent software baselines, and easy and immutable deployments are all critical to bringing expected patch times down to acceptable levels.

Appendix B: Principles of Cloud-Oriented Security Protections

As noted in this Report, the Federal Government has traditionally focused its Government-wide information security efforts on protecting network boundaries; however, instead of emphasizing physically consolidated security at the perimeter, such as in the current Trusted Internet Connections (TIC) model, a data-centric approach emphasizes placing protections closer to the services and information systems in which sensitive data is stored and accessed. This gives agencies flexibility in the approaches they choose. For modern services hosted in the cloud, agencies can place security protections directly in front of each service and allow direct connections from the public internet. For services hosted in legacy data centers, such capabilities may not be available, in which case the agency can still rely on perimeter security as they pursue options to modernize their system architecture.

There is no one right way for an agency to operationalize security protections in Cloud Service Providers (CSPs), and some features and approaches may need to be optimized for the particular cloud service provider in use. Agencies should ensure any CSP they choose meets the security capabilities outlined by FedRAMP. The approach in this appendix applies to cases wherein an agency is directly operationalizing software in a cloud-hosting environment. This does not apply to Software as a Service (SaaS) applications operated in full by vendors, as their security approaches will be vendor-specific.

Agencies could take the following approach to designing security protections in a cloud-based application stack:

- An agency could separate their security stack from their application stack within their cloud provider. In whatever way this separation occurs, agencies should maintain the principle that a compromise of the application being protected should not automatically lead to compromise of the security stack being used to protect that application and vice versa;
- Incoming traffic could be routed through the cloud provider's commodity virtualized load balancers, used to obtain a carbon-copy of the data, to a set of virtual security appliances. These virtual security appliances would process incoming traffic "on path," meaning that incoming requests are blocked on the ability of the security appliances to process them. Since putting any devices "on path" of existing traffic has significant reliability, security, and performance implications, the choice of security functions for this purpose must be warranted by the sensitivity of the application. Lower sensitivity applications likely warrant few, if any, "on path" request processing services;
- These virtual appliances could themselves implement most of the security functions described by existing TIC policy, including intrusion detection, filtering, and logging. Importantly, these virtual appliances must be horizontally scalable so that any number of instances can handle as much traffic as the service might receive; and
- After the traffic is processed by the virtual security appliances, it exits the segregated security zone. It is then sent to the application's load balancer to be processed normally by the application.

An example diagram showing data-centric security in a cloud provider is shown in **Figure 1**.

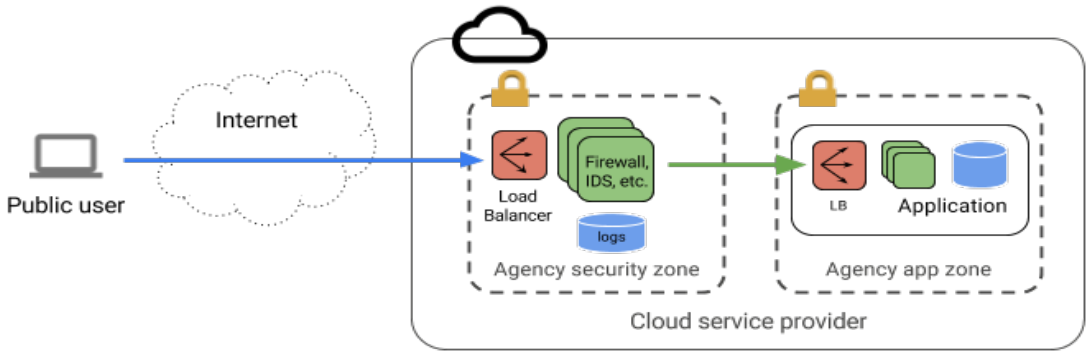


Figure 1

This data-centric application security layer could be implemented directly by an application team, or it could be run by an agency as an internal shared service for all applications hosted within a particular cloud provider. It could also be possible for a sufficiently responsive agency team to provide this layer as a shared service to multiple agencies who utilize the same cloud provider.

To achieve centralized visibility for agency security teams, this data-centric application security layer should send logs and alerts in real time to centralized aggregation systems that process security information and events. These centralized aggregation systems could be co-located in the same cloud provider as the applications from which they are aggregating information. They could also aggregate logs and network flow information received from the cloud service provider itself. One operational approach for doing this is described in the Security Operations Center as a Service section of this report.

Government-Wide Visibility and Classified Indicators

Some Government-specific security functions, such as the intrusion detection and prevention capabilities of 6 U.S.C. § 151, currently offered as EINSTEIN, would not be automatically fulfilled by commodity solutions. Some needs, for example, can only be addressed with classified indicators. This produces a challenge for agencies, as these classified indicators can only be stored in data centers meeting very specific security requirements. For most systems, however, these Government-specific functions, such as EINSTEIN 1 and EINSTEIN 2, do not leverage classified indicators or need to be physically “on path” for network traffic and incoming requests. Instead, the virtual appliances in the data-centric security layer could create a copy of relevant traffic or logs and send a stream to a nearby location (perhaps operated by DHS as part of the intrusion detection and prevention capabilities of 6 U.S.C. § 151) where these Government-specific security functions can be performed in the background. The original copy of the traffic continues to flow to the cloud provider unless, depending on the capability at issue, an alert is generated from the intrusion prevention system. This achieves visibility and detection

of classified threats without sacrificing the major benefits of adopting modern cloud architectures. A diagram of how this may look is represented in Figure 2.

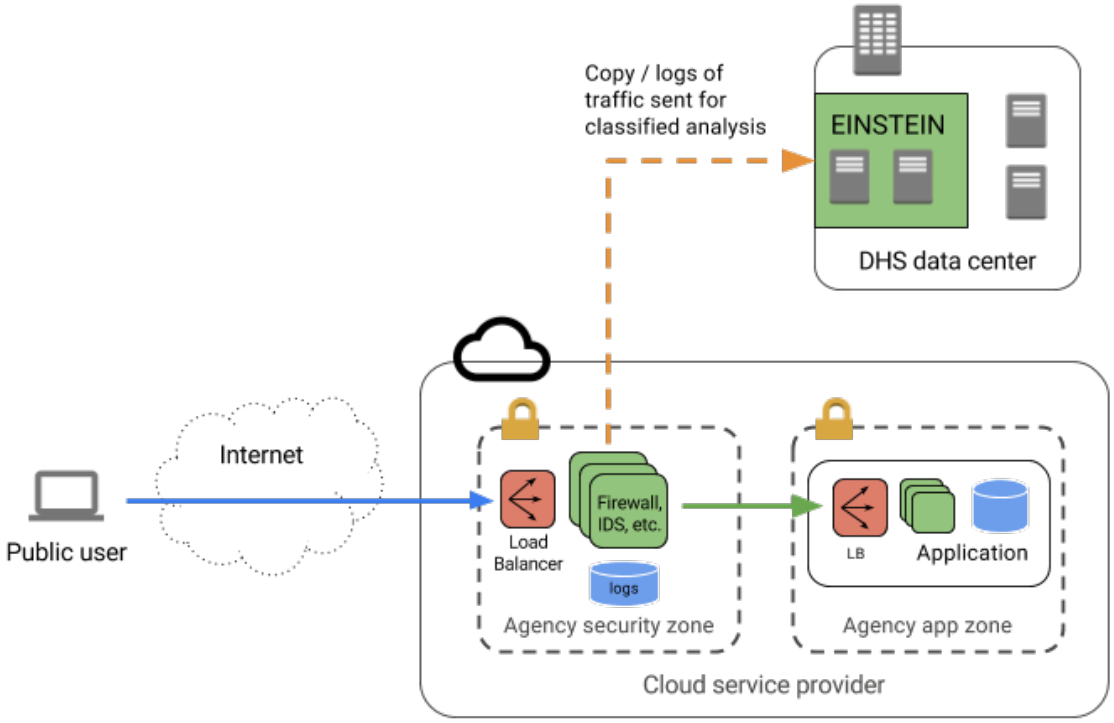


Figure 2

DHS should also consider evolving NCPS's intrusion prevention capabilities program to include the ability to receive and act on additional application layer traffic. In its current form, EINSTEIN 3A does not process most web traffic, because it only examines email and domain name server.

The data-centric approach outlined above also allows a more nuanced approach to protection, allowing security teams to focus their efforts on the systems that need it most. For low-impact systems that only store public data, it is likely unnecessary to split off traffic for classified analysis. For high-sensitivity systems with very valuable private data, it may be useful to require more security measures, such as waiting for classified analysis to be complete before passing traffic along to the application.

Proportionate Security

While the protections described in this appendix can be useful to many applications, the Federal Government should focus its limited security resources on its highest-value assets. All security protections come with a cost: any security services "on path" can impact reliability and performance, add complexity to system operations, and could have vulnerabilities that would be used against the applications they are intended to defend. Even "off path" security services that do not process data in real time, such as classified indicators and services that provide

Government-wide visibility, add complexity as well as oversight and compliance costs to system operation.

For the Government's security protections to be most effective, they should be deployed on systems whose data is worth such a sustained and sophisticated defense, such as HVAs. Systems that contain information that would have a low impact if compromised should instead be optimized for agility and availability, thus freeing security resources for more sensitive systems. An isolated system with no sensitive information therefore might merit a more streamlined architecture. **Figure 3** shows how a low-impact system may serve requests directly:

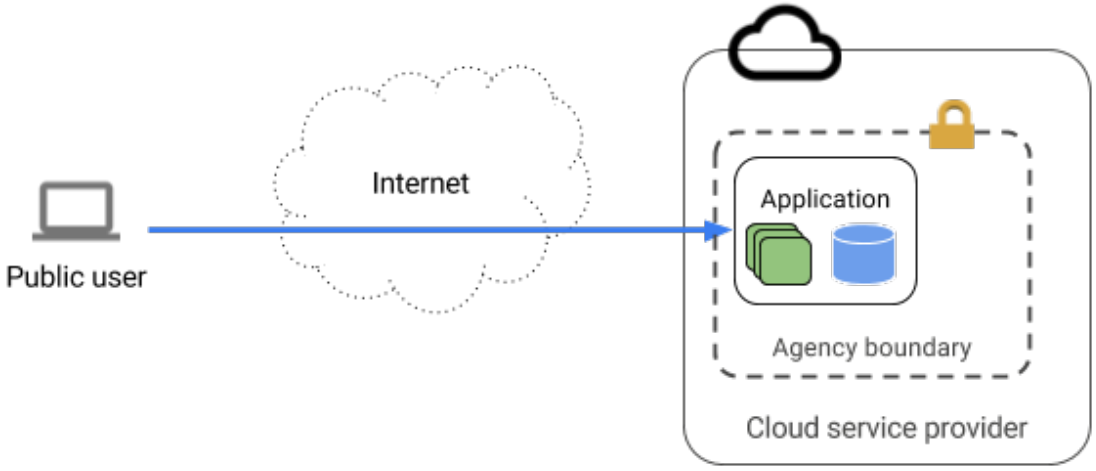


Figure 3

Appendix C: Challenges to Implementing Federal-Wide Perimeter-Based Security

Today, the Federal Government applies a defense-in-depth strategy to protect its systems that includes agency and DHS-provided protections at various levels. But, at the same time, Government-wide programs overly rely on a perimeter-based security model to protect the Government's networks and information systems. This model, formalized in OMB Memorandum M-08-05, *Implementation of Trusted Internet Connections (TIC)*, focuses on standardizing security at the network boundary through consolidation of external access points. Under this model, the Government has required agencies to reduce external connections, to a target of 50, and route their traffic through this limited number of secure gateways. These gateways apply common intrusion detection and prevention capabilities under DHS's National Cybersecurity Protection System (NCPS). NCPS consists of three sensor capabilities (collectively referred to as EINSTEIN), as well as a set of analytic tools used by cyber analysts to find, identify and categorize cyber threat activity. [29]

The NCPS sensor suite is deployed in three iterations: EINSTEIN 1 (E1), which captures and analyzes network flow information; EINSTEIN 2 (E2), which incorporates intrusion detection technology that scans the content of network communications to identify and alert to known indications of malicious activity; and EINSTEIN 3-Accelerated (E3A), which detects and blocks malicious activity through DNS sinkholing and email filtering.

This perimeter-based architecture has created several challenges, specifically regarding adoption of commercial cloud and mobile technologies. Additionally, signature-based detection and protections systems provide value, but are not enough to combat the full spectrum of advanced persistent threats that rapidly change attack vectors, tactics, techniques, and procedures.[30, 31] All of these challenges are acknowledged and understood by DHS, and efforts are underway to address these specific issues.

As an overarching effort, DHS has undertaken a cybersecurity architectural review of Federal, Civilian, and Executive Branch infrastructure to capture empirical data, which will be used to determine the efficacy of individual and collective groupings of capabilities against specific threats to that architecture. This data will then be used to guide the evolution of DHS cyber program capabilities, to include NCPS and the CDM program.

In addition to the holistic architecture review, DHS has continuously assessed its programs to determine if the program investments they are making are appropriate. As part of this continuous assessment, DHS has identified several challenges that must be addressed to improve and deliver value to its Federal Executive Branch stakeholder community. These challenges include:

1. Cloud Security and Situational Awareness
2. Encrypted Network Traffic

---

[29] See Footnote 9.

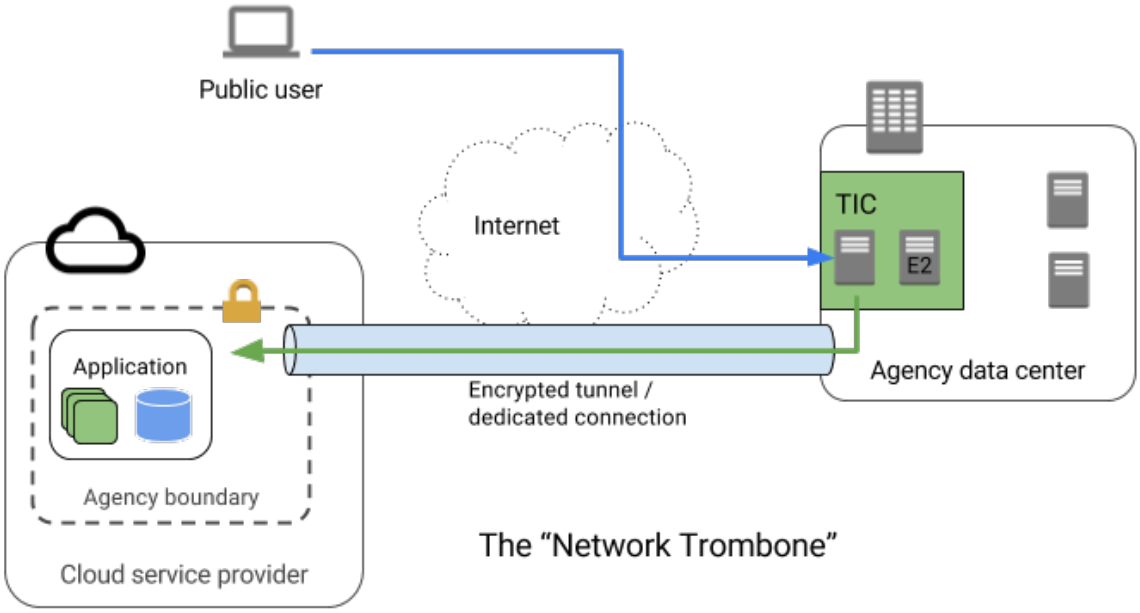
[30] DHS Office of the Inspector General, *Implementation Status of EINSTEIN 3 Accelerated*. March 2014.

[31] U.S. Government Accountability Office, Report 16-294, *DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of its NCPS*. January 2016.

3. Overreliance on Static Signatures
4. Use and Value of Classified Indicators

Cloud Security and Situational Awareness

Federal agencies have started to embrace the use of cloud services to include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), which has the promise to move much of the Federal Executive Branch's computing and data to commercially available cloud environments, outside of traditional network boundaries. In doing so, the emphasis on protecting and monitoring perimeter connections of trusted networks at a limited number of physical TIC access points has introduced performance degradation. This has discouraged agencies from fully adopting cloud services, and undermines many of their key benefits such as reducing costs, flexibility, time-to-deploy, and availability and reliability. An example of a current network routing challenge for agencies that have adopted cloud services is an agency that has implemented a public-facing web service must route user traffic through a limited number of physical TIC access points for inspection, which in turn introduces latency. The diagram below illustrates how this approach is currently implemented, in a phenomenon known as "the network trombone," which constrains the benefits of cloud services by forcing users to route traffic through a physical network location rather than being able to connect directly to the cloud service.



To address this situation, DHS has engaged with three large cloud service providers to determine how DHS may gain the insight and situational awareness from within the cloud that is similar to the information that is gained from its E1 and E2 sensors that are deployed at the TICs. The focus of this engagement thus far has been the collection of internal cloud log data, specific to the agency application and data that could be fed back to DHS to provide a similar level of situational awareness to DHS cyber analysts.

Encrypted Network Traffic

As the use of cloud and web services continues to expand, so has the use of network transport security in the form of encrypted tunnels between end users and their applications and data. The use of transport encryption is critical for secure communications, but limits what is visible to a perimeter-based monitoring system such as E1 or E2. The amount of network traffic that is encrypted that passes through E1 and E2 sensors has increased over time, with 47 percent of all traffic being encrypted as of December 2016. This continued growth of encrypted network traffic has limited the functionality and usefulness of E1 and E2 sensors and has made it difficult for DHS to inspect this traffic for cyber threats. For DHS E2 sensors, this means that DHS signatures are unable to inspect the content of network communications and alert on malicious content.

Continued growth in encryption is both beneficial and inevitable, and DHS has commissioned research to determine potential architectural, technical, and policy mitigation strategies that could provide DHS with both the protection and situational awareness for encrypted traffic. Some of the mitigation strategies currently under evaluation include:

1. **Sensor Placement**. This involves relocating the E1 and E2 sensors where the traffic is decrypted (e.g., endpoints of an encrypted tunnel). In the cases of virtual private network tunnels, one could place sensors outside of encrypted areas. For cloud environments, investigation is needed to determine how these sensors could be virtualized and placed in physical or virtual locations where Government applications and data exist.

2. **Man-In-The-Middle (MITM) Interception**. This involves deploying MITM technologies that decrypt traffic, inspect it, and re-encrypt it, by placing a proxy along the network path. This proxy falsely pretends to each side to be the other side of the communications. Network proxies that intercept Transport Layer Security (TLS) traffic via MITM are commercially available. Usually this requires local clients to have blanket trust of this proxy.

3. **Key Escrow**. This involves gaining access to decryption keys (e.g., as part of a broader certificate management system and architecture). A key escrow approach requires clients to register keys with a trusted third party.

Overreliance on Static Signatures

The use of signatures, or software code that inspects network traffic to look for known content, ports, and protocols, has been a fundamental part of cybersecurity practice. Similar to how anti-virus software works, intrusion detection and prevention technologies inspect traffic to look for matches against signatures of known malicious content or behavior. Although signature-based technology is widely accepted as an effective and necessary piece of cyber defense, it is not enough to protect against the most advanced and persistent threats facing the Government today. NCPS uses signatures within their E2 intrusion detection and E3A prevention capability areas. In recognition of the limitations of signature-only systems, DHS has been piloting an

anomalous analytics capability that leverages artificial intelligence to detect malicious activity across networks that will allow DHS to both respond to previously unidentified incidents. DHS can then rapidly generate new signatures for both EINSTEIN sensors and agency defenses to protect the Government from those threats. DHS has seen some early success from this pilot and is planning to build a production-grade system that could be deployed at various points across the .gov architecture, both inside and outside agency network and computing enclaves.

Use and Value of Classified Indicators

The use of signatures in intrusion detection and prevention systems are based on pieces of information known as cyber threat indicators. These "indicators" can be any piece of observable information about the network traffic such as an Internet Protocol (IP) address, domain name, or file hash, that may indicate whether the traffic entering or exiting a network may be suspicious or malicious. DHS sources its indicators from multiple sources to include in-house analysis of Government traffic, commercial and open-source cyber threat data, and the intelligence community. Although all of the signatures within the E2 system are unclassified, significant portions of the signatures in the E3A intrusion prevention capability are classified. The use of classified indicators and signatures within the E3A system has been a long-standing challenge for the NCPS program because of the unprecedented way in which classified information is placed on unclassified networks for the purposes of protecting unclassified .gov network traffic. The continued use of classified information in E3A has been recognized as a cost and schedule driver, as well as limiting the range of technical capabilities available. Moreover, the use of classified information has limited the ability of DHS to engage and communicate with the agencies it helps to protect because not all agencies have personnel with the appropriate security clearances to discuss the indicators or the alerts that are generated by the system. To address this issue, DHS has commissioned a study to understand the value of using classified indicators within E3A to determine if their use should be continued, or if DHS and the agencies would be better served by using only unclassified information.

Appendix D: Acquisition Pilot: Change the Buying Strategy to Government-As-One-Purchaser

The Government must pursue new acquisition strategies for cloud email and collaboration licenses. In furtherance of this objective, pilots such as the example outlined in this Appendix may be executed to decrease the administrative acquisition burden, specifically for smaller agencies who cannot leverage large volume discounts or who have acquisition workforce constraints. Additional pilots to leverage the Government as one purchaser and speed cloud adoption may include the ability to purchase cloud services on a consumption basis and coordinated purchasing to obtain tiered-based pricing.

Several challenges must be overcome in the acquisition cycle in order to comply with EO 13800 and facilitate shared services, such as cloud email. Budgets are constrained by yearly appropriations, and agencies work autonomously, which reduces the Government's ability to look at its purchasing as a whole. Legacy procurement and security regulations, coupled with lack of top down guidance for the logistics of a Government-wide migration to cloud email challenge cloud adoption.

By creating virtual "street corners" for cloud email providers the Federal Government can use competing market forces to drive Government-wide volume pricing as a lever to speed migration. This will apply Hotelling's Law of spatial competition, wherein Government's potential purchasing power will be used to negotiate tiered pricing agreements directly with the providers and result in publicly displayed price points, total number of licenses purchased, and the remaining number of mailboxes that need to be migrated. This volume pricing would serve as the base rate for any license purchased by the Government.

Public Dashboard Example (Cloud-Based E-mail)*

In this scenario, data would be recorded and displayed publicly with the current negotiated pricing tiers, along with any incentive pricing based on other factors such as the company's quarterly sales cycles.

Cloud Email Provider A	Quarter/ Price per user/month
Tier 1: 1-5,000 licenses	Q1-3: 2% discount
	Q4: 2.5% discount
Tier 2: 5,000– 10,000 licenses	Q1-3 2.7% discount
	Q4: 3.0%
Tier 3: 10,000 – 50,000 licenses	Q 1-4: 3.2%

**These numbers are fabricated for this example only.*

A running total of the licenses purchased would be displayed so that at any time, end users would know the price point. This would be validated with the companies for the official count.
Publicly Displayed Information Example:

As of 6/29/17 Total Licenses purchased Government-wide: 1,345,000

Pricing Level= Tier 3, Q2 = $3.2% discount per user/month

Total mailboxes to migrate: 3,000,000

The objectives and expected outcomes would include a more constructive and mutually-beneficial ecosystem with private sector companies, better and more transparent pricing for Government agencies, and an increased variety of available secure solutions. This would also lead to more consistent implementation and configurations across the Federal enterprise. Lastly, this would incentivize agencies with smaller budgets to adopt cloud email earlier.

Assumptions

This assessment relies on the following assumptions:

- Industry and private sector companies are not only willing to come to the table, but to actually collaborate with the Federal Government in pursuing this new approach to contracting;
- Industry must be willing to negotiate fair and reasonable tiered volume pricing that will be made public. Departments, agencies, and industry must agree on metrics and public reporting and tracking of agency adoption of cloud email adoption;
- Agencies must also be active in timely reporting of their data, which will be displayed publicly, in order to ensure as specific volumes are reached, discounts are provided;
- The Government has the ability to negotiate a Manufacturer's Agreement that will be accepted by agencies; and
- This approach is platform agnostic, any cloud-based email provider may be eligible to participate; agencies will still need to follow competition rules as required to place orders.

Why This Works

A common strategy for many chains is to locate near a competitor. For example, you will almost always see a CVS near a Walgreens or a Burger King near a McDonalds. You will see food chains across the street or next to each other in almost any city in the United States. The thinking is that if it works for the competitor, it will likely work for you. Studies have shown repeatedly that as chains sprout up in adjacency, volume also goes up. This strategy is commonly known as the Nash Equilibrium, a solution concept of non-cooperative competition involving two or more "players," where each player knows the equilibrium strategies of the others and no one has anything to gain by changing their own strategy.

Creating the Marketplace with Hotelling's Law: In simple terms, Hotelling's Law determines that businesses selling similar products tend to locate as close as possible in order to maintain the maximum amount of market share possible. Creating a public display and accountability to the total Government spend for the different types of cloud email and the number of mailboxes left to be migrated will create this marketplace.

This strategy also takes into account that re-sellers would still be able to sell these licenses under existing GSA Schedules and Government-wide Acquisition Contracts (GWACs), or NASA SEWP contracts; however, they would be required to use the current price point, record the sale into the dashboard, and make their re-seller fees transparent to Government as the differentiation in

competition. Ultimately, this will save business development and contract negotiation time and effort between the email providers and the re-sellers, which will drive down the overhead fees the Government has to pay.

Services, configurations, and prices all negotiated openly and reported publicly will not only ensure the most competitive rates for Government, but also create an optimal strategy for the vendors themselves. This dis-incentivizes vendors from focusing on the highest possible price point for their services and, instead, refocuses the competition on performance and quality of the offerings as a distinguishing factor.

Pilot to Test the Hypothesis

The steps outlined below would be used to test the theory that this would change the way we buy these services and establish a shared service approach to license purchasing. This is not the full implementation plan which will provide more details for how and when these general steps will be accomplished. The implementation plan will address pilot success criteria to include input and feedback from agencies and industry which may change the course of the outcome.

Get Industry Buy-in and Feedback. Capitalizing on the recent success of the IT CEO Summit, the Office of American Innovation will call a follow-up summit with interested cloud providers to discuss the proposal. The goal would be to determine whether CSPs would be willing to participate in a pilot with the Federal Government.

Measure the Market. A prerequisite to all other actions is to obtain an accurate measurement of the market need in terms of agencies that have not yet transitioned to cloud email solutions. While we have clear data on implementation among the CFO Act agencies, currently there is no definitive data source of small and independent agencies adoption of cloud email. In order to negotiate effectively, knowing the size of the market is imperative, therefore we need a data call to all agencies regarding their current email contracts, prices, and number of mailboxes, etc.

Establish Focused Pilots with Partners. ATC and OMB will work with a small group of agencies to establish a pilot program to examine the impact of the process changes being proposed. Additionally, they will lead the creation of a series of support groups that would deploy to agencies to provide technical, acquisition, and migration assistance and report to ATC on the progress of the pilots. This will include a strategy to minimize the burden on early adopters, potentially through price redetermination terms, modular contracting methods, or collaborative purchase agreements.

Create a Reporting Mechanism with Agencies and Industry. The Federal Government requires that accurate and up-to-date data around the current state of both cloud and on-premises email adoption be reported by agencies so as to develop a baseline against which agency progress may be tracked. Industry sign-off on transparent reporting of units and volume pricing is essential to the success of this proposal. Without it, this strategy will ultimately fail. This is the foundation for achieving Nash Equilibrium for both the Federal Government and industry.

Notional Metrics of Success

- At least one cloud-based email service provider has signed up to negotiate a memorandum of understanding within 90 days of the report being published, which would allow the Government to begin capturing FY 2018 spending on cloud email migrations;
- At least two agencies have signed on to pilot the proposed dashboard and provide reporting and acquisition of cloud email licenses under this effort; and
- Within 30 days of qualified purchases, agencies or re-sellers will record the sale in the dashboard.

Appendix E: Legal Considerations

Introduction

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* requires this report to "describe the legal . . . considerations . . . relevant to . . ." transitioning agencies to consolidated network infrastructures or shared services. Exec. Order No. 13,800, 82 FR 22391, § 1(c)(vi)(B)(2) (May 11, 2017). This appendix, along with the report itself, does so. The report suggests increased use of consolidated network architectures and shared services. Generally, Federal law contemplates that agencies control their own systems and information either directly or through contract. Moving to consolidated network architectures, commercial cloud and shared services generally involves moving away from agency control and thus tends to increase tension with relevant law and requires greater analysis and legal documentation. While additional legal review and documentation would need to be performed during any eventual development of the consolidated network architectures, commercial cloud, and shared services based on their exact facts, implementation of the report's recommendations can likely be achieved within existing law in most instances, as long as they are designed with a view toward satisfying applicable legal requirements. A summary of some of the main areas of law and legal issues implicated by this report are discussed below.

The Federal Information Security Modernization Act of 2014 (FISMA)

The Federal Information Security Modernization Act of 2014 (FISMA) and later amendments are codified in subsection II of chapter 35 of title 44 of the U.S. Code. These provisions, which we will refer to here as FISMA, create a whole-of-Government approach to Federal information security[32] pursuant to which OMB oversees agency information security policies and practices; DHS administers implementation of these policies and practices for Federal, civilian, executive-branch agencies, including by assisting agencies and providing certain Government-wide protections; and agencies are responsible for providing information security protections commensurate with the risk and magnitude of the potential harm to their agency information and information systems. *See* 44 U.S.C. §§ 3551-3558. FISMA also requires agencies to implement a minimum set of information security controls and techniques, assess the effectiveness of these controls, comply with NIST standards, DHS directives, and OMB policies, and report certain cybersecurity information to DHS, OMB and to Congress. The consolidated network architectures, commercial cloud, and shared services recommended in this report will need to provide levels of security and transparency that enable agency heads to ensure compliance with FISMA and its related requirements, while also providing technical solutions that fit the needs of multiple agencies.

[32] In FISMA, the term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—
(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
(C) availability, which means ensuring timely and reliable access to and use of information.

The Homeland Security Act's Federal Intrusion Detection and Prevention System

The Homeland Security Act, as amended, requires DHS to "deploy, operate, and maintain" and "make available for use by any agency" capabilities to detect cybersecurity risks in agency network traffic and take actions to mitigate those risks. 6 U.S.C. § 151(b)(1). DHS currently provides these capabilities through its EINSTEIN program and, as required by law, ensures all retention, use, and disclosure of information obtained through EINSTEIN occurs only for the purpose of protecting information and information systems from cybersecurity risks. *See id.* § 151(c)(3). Federal law also requires agencies to apply these capabilities to "all information traveling between an agency information system and any information system other than an agency information system." *Id.* § 151, note. Because this statutory mandate defines "agency information system" as any "system owned or operated by an agency," the statutory mandate itself does not always require agencies to apply those capabilities to systems operated by contractors. But existing policy requires broader application of EINSTEIN, and DHS and agencies can choose to apply the capabilities to contractor-operated systems.

Privacy Statutes

There are many provisions of law and regulation that that protect personally identifiable information by, for example, limiting access. *See, e.g.*, U.S. Const. amend IV; Fed. R. Crim. Pro. 6(e)(2)(B) (grand jury confidentiality rule); 5 U.S.C. § 552a (Privacy Act of 1974); 26 U.S.C. § 6103 (restrictions on access to tax return information); 13 U.S.C. § 9(a) (Census confidentiality statute); 18 U.S.C. § 2511 (Wiretap Act); 6 U.S.C. § 151 (DHS's Federal Intrusion Detection and Prevention System). Personnel operating consolidated network architectures, commercial cloud, and shared services described in this report will sometimes require access to such information. Technical capabilities and administrative processes will need to be developed to enable compliance with the laws and regulations applicable to each type of information. This will require a significant role for SAOPs and agency privacy programs.

Request for Information from Third Parties

Agencies receive requests for information in their possession through various means, including, for example, Freedom of Information Act (FOIA) requests, Privacy Act requests, congressional requests, Government Accountability Office audits, Inspector General inquiries, court proceedings, requests from the White House or other agencies, and other legal process. Legal agreements between shared service providers and client agencies will be required to define who will be responsible for responding to such requests when the information resides in a shared service in a way that satisfies legal requirements and provides agencies with sufficient control over their own information. Likewise, agency notices and regulations should adequately inform the public and others who might make requests of the appropriate procedures for accessing information.

The Federal Information Technology Acquisition Reform Act (FITARA)

The Federal Information Technology Acquisition Reform Act (FITARA) increases the authority of agency Chief Information Officers to play a significant role in the planning, programming, budgeting, management, governance and oversight of Federal information technology. 40 U.S.C. § 11319(b)(1)(A). FITARA is consistent with a move toward consolidated network architectures, commercial cloud, and shared services and enhances the legal authority for agency CIOs move in that direction. Among other actions, FITARA and associated policy require agencies to implement data center consolidation strategies that support (i) movement of information technology infrastructure to the as-a-service model and (ii) transition to the cloud. *See* 44 U.S.C. § 3601, note.

Procurement and Fiscal Considerations

Transitioning to consolidated network architectures and shared services requires consideration of how those products or services will be acquired and funded. In order to consolidate and share services with each other, Federal agencies will need to enter into Interagency Agreements or other appropriate agreements with each other that outline the parameters of their relationship and the applicable authorities that govern, for example, the acquisition of the products or services, how they will be shared and utilized by the parties, and how they will be funded and reimbursed. The specific authorities may vary depending on the circumstances and agencies affected, but may include:

- The Economy Act, 31 U.S.C. § 1535, which authorizes Federal agencies to enter into agreements to obtain supplies or services from another Federal agency and requires full reimbursement.
- Agency-specific authorities. For example, 40 U.S.C. § 501 authorized GSA to procure and supply property and services for executive agencies. The funding source utilized in conjunction with 40 U.S.C. § 501 will depend on which office within GSA is providing the property and services, but may include the Acquisition Services Fund (40 U.S.C. § 321), a Working Capital Fund, or other specific authorities. In general, full reimbursement will be required unless specifically authorized otherwise. In an example of such a specific authorization, 44 U.S.C. § 3553(b)(6)(B) authorizes DHS to "upon request by an agency, deploy[], operate[], and maintain[] technology to assist the agency to continuously diagnose and mitigate against cyber threats and vulnerabilities, with or without reimbursement."

Appendix F: Summary of Recommendations

#	Responsible Party/ies	Action Required	Submitted to	Timeline (Following issuance of the report)
Network Modernization & Consolidation Prioritize the Modernization of High-Risk High Value Assets (HVAs)				
1	Department of Commerce (NIST)	Provide a plan for revising Federal Information Processing Standard (FIPS) 199 and FIPS Publication 200. The plan must include: ● Proposed update to any other relevant NIST Special Publications to support the transition of agency compliance efforts away from low-impact systems and toward high-impact systems; The updates should include the use of the Cybersecurity Framework, and, where appropriate, incorporate lessons from other control and compliance frameworks. The updates should review security requirements for other frameworks and system approval processes, and assess the use of overlays of these frameworks into the proposed updates of the relevant Special Publications.	OMB	30 days
2	DHS and NIST	DHS - Provide a report which identifies common areas of weakness in Government HVAs. NIST – Provide a plan to improve cryptographic agility in the Federal enterprise.	OMB	60 days
3	OMB (in coordination with DHS)	Update the Federal Information Security Modernization Act of 2014 (FISMA) metrics as well as the Cybersecurity Cross-Agency Priority (CAP) Goal metrics to focus on those critical capabilities most lacking in agencies. Focus review and oversight efforts on driving progress on these capabilities, specifically focused on HVAs.	Government-wide release	90 days
4	DHS	Work with agencies, including by issuing direction when appropriate, to support mitigation actions to address common areas of risk identified in the Report to the President on Risk Management in accordance with their authorities.	Government-wide release	90 days
5	OMB (in coordination with DHS)	Develop a strategy for an approach to improve lines of authority and operating procedures across agencies to reduce enterprise risk and coordinate responses to cybersecurity incidents.	[For internal action]	120 days

6	Agency CIOs, CISOs, and SAOPs	● Review their latest submission of HVAs and make any necessary changes to reflect the latest information on system prioritization in tandem with the assessments made under their risk assessments as part of Section 1 of Executive Order 13800.	DHS and OMB	150 days
7	DHS, OMB, and the NSC	Review HVA lists submitted to DHS by Federal agencies and produce a prioritized list of systems for Government-wide intervention. Six HVAs will be selected to receive centralized interventions in staffing and technical support.	President's Management Council	180 days
8	Any agency that has an HVA identified as having a major or critical weakness in either a risk assessment, RVA, SAR, or agency sponsored review	Identify a remediation plan, including a proposal for accelerating modernization within one year and identification of impediments in policy, budget, workforce, or operations. The plan should: ● Maximize use of shared IT services and consider application and data-level protections and the use of commercial cloud-based architectures; and Prioritize existing financial and human resources and should identify other systems of concern that may suffer from similar issues not categorized as HVAs.	OMB and DHS	180 days
9	Any agency that has an HVA identified as having a major or critical weakness in either a risk assessment, RVA, SAR, or agency sponsored review	Identify a remediation plan, including a proposal for accelerating modernization within one year and identification of impediments in policy, budget, workforce, or operations. The plan should: ● Maximize use of shared IT services and consider application and data-level protections and the use of commercial cloud-based architectures; and ● Prioritize existing financial and human resources and should identify other systems of concern that may suffer from similar issues not categorized as HVAs.	OMB and DHS	180 days
10	DHS (in coordination with OMB, USDS, and GSA)	Provide hands-on technical assistance to agencies in bolstering protections for systems identified through the process outlined above as having the greatest need for modernization.	[For internal action]	180 days
11	DHS	Expand the availability of DHS RVAs and SARS for agency HVAs and work with OMB to refocus these engagements to concentrate on hands-on technical engineering interventions. Work with GSA to expand the visibility, offerings, and agency use of the Highly Adaptive Cybersecurity Services Special Item Numbers on IT Schedule 70.	[For internal action]	180 days

12	OMB (in coordination with DHS, GSA, Federal agencies, other stakeholders)	Capture standard operating procedures for the protection of HVAs. Develop a playbook that agencies can leverage to expand this approach to other systems in a prioritized, risk-based fashion.	Government-wide release	365 days
Network Modernization & Consolidation Modernize the Trusted Internet Connections (TIC) and National Cybersecurity Protection System (NCPS) to Improve Protections, Remove Barriers, and Enable Commercial Cloud Migration				
13	OMB	Submit a data call to agencies requesting submission of both in-progress and pending projects for cloud migration.	Government-wide release	30 days
14	Agencies	Respond to OMB data call. Propose a cloud migration plan that highlights needed changes to requisite policies and capabilities to facilitate faster migration.	OMB	Commensurate with timelines in the data call request
15	GSA, DHS, OMB, NSC, USDS, and other relevant parties	Review agency data call responses.	[For internal action]	60 days
16	OMB	Provide preliminary update to TIC policy that introduces 90-day sprint during which projects approved by OMB will pilot proposed changes in TIC requirements.	Government-wide release	60 days
17	Agencies	Require collection of metrics that will be used to ensure that any proposed policy change does not introduce an unacceptable level of cybersecurity risk.	OMB, DHS, GSA, NSC	90 days
18	GSA, DHS, OMB, USDS, NSC	Kick off a 90-day sprint to validate particular case studies for Category 2 cloud migration projects.	[For internal action]	90 days
19	GSA, DHS, and OMB	For category 3 cloud migration projects, work with agencies to evaluate whether there are common features or capabilities that could be provided efficiently, effectively, and securely by CSPs. This analysis will serve as an input to the FedRAMP JAB's prioritization of high-baseline CSP offerings available to agencies wanting to migrate high-impact data to the cloud.	[For internal action]	90 days
20	OMB, GSA, and DHS	Using information gathered from previous actions, proceed with rapid updates to TIC policy, reference architectures, and NCPS operational models to facilitate outcomes in commercial cloud.	Government-wide release	180 days

Network Modernization & Consolidation Consolidate Network Acquisitions and Management				
21	DHS	Provide GSA and agencies with baseline configuration guidance for Managed Security Services capabilities offered under EIS.	GSA	60 days
22	GSA, in coordination with DHS	Develop a comprehensive acquisition strategy that provides a feasibility assessment and roadmap to accomplish the following: ● Provide a path for all small agencies to more easily and cost-effectively utilize EIS services; ● Review current security capabilities currently offered under MTIPS to ensure the capabilities provide adequate security within the current threat environment; ● Identify additional areas of opportunity outside of EIS to consolidate acquisition of cybersecurity services and products; and ● Determine the feasibility of establishing a centralized acquisition support function within GSA capable of performing cybersecurity-related contract management activities for small agencies.	Government-wide release	90 days
23	GSA	Support small agencies in the transition to EIS by consolidating requirements for small agencies.	[For internal action]	None given
24	GSA	Provide guidance to small agencies on how best to leverage its cross-agency acquisition in order to optimize small agencies' investments and management throughout the procurement process.	Small & independent agencies	None given
Shared Services to Enable Future Network Architectures Enable the Use of Commercial Cloud Services and Infrastructure				
25	OMB	Issue data call that will have agencies identify systems that may be ready for cloud migration and can be migrated securely but have not yet migrated due to perceived or encountered difficulties.	Government-wide release	30 days
26	Agencies	Respond to OMB data call.	OMB	Commensurate with timelines in the data call request
27	OMB and GSA	Review the impediments to moving to the cloud outlined by agencies and will prioritize an infusion of technical talent, capital, and updated security policy (developed iteratively to solve agency-specific issues) as needed to enable prioritized cloud migrations	[For internal action]	Conclusion of data call

28	GSA (with OMB)	Work with volunteer agencies to pilot new initiatives to improve the speed, reliability, reusability, and risk acceptance transparency for cloud-based SaaS and shared services ATOs. Based on the combined efforts, including lessons learned and best practices for extending these pilot activities to a Federal civilian-wide scale, GSA will work with OMB to develop any necessary plans or policy for promoting these initiatives and any other innovative FedRAMP, shared services, or agency-specific efforts across the Federal enterprise.	Government-wide release	90 days
29	OMB, in coordination with DHS and other Federal partners	Update the Federal Cloud Computing Strategy ("Cloud-First"), which will provide additional guidance to agencies on the most impactful use cases for cloud adoption and how best to conduct appropriate operational security in cloud environments.	Government-wide release	120 days
30	OMB	Conduct a thorough review of all relevant policies pertaining to IT modernization, cloud migration, infrastructure consolidation, and shared services, among others, and initiate revisions, rescissions, or other rapid policy updates that may improve the ability of agencies to modernize effectively, securely, and efficiently. If necessary, OMB will issue further guidance that will augment and enhance existing Federal technology and information security policy.	Government-wide release	120 days
31	OMB, in coordination with the FAR Council, GSA, and DHS	Develop clauses that define consistent requirements for security, privacy, and access to data for use in cloud contracts.	Government-wide release	120 days
32	OMB, working with the FAR Council, GSA, and DHS	Assemble a tiger team to develop a set of proposed acquisition statutory and regulatory changes that specifically target and help to achieve the modernization goals outlined in this report. The tiger team will look to leverage regulatory reform efforts being conducted under legislative and executive order direction, while at the same time (i) maximizing the use of commercial products and services; (ii) Promoting competition; (iii) Minimize administrative operating costs; (iv) Conduct business with integrity, fairness, and openness; and (v) Fulfill public policy objectives. The tiger team's recommendations shall be fully coordinated with the appropriate stakeholders before being adopted.	Government-wide release	180 days
	Shared Services to Enable Future Network Architectures Accelerate Adoption of Cloud Email and Collaboration Tools			

33	OMB	Conduct a data call to agencies regarding their current email contracts, prices, and number of mailboxes.	Government-wide release	30 days
34	Agencies	Respond to OMB data call.	OMB	Commensurate with timelines in the data call request
35	OMB	Convene a task force of agencies to finalize a set of requirements for both low and moderate security postures for email and cloud collaboration.	Government-wide release	30 days
36	OMB	Establish a comprehensive strategy for driving the accelerated migration of agency email and collaboration tools to the cloud for departments and agencies who have still not adopted cloud-based email.	N/A	60 days
37	OMB	Issue updated identity policy guidance for public comment.	Government-wide release	75 days
38	OMB	Assemble Acquisition Tiger Team, charged with drafting and disseminating a "quick start" acquisition package that can help agencies facilitate rapid license and migration service acquisitions. The package would include: ● Market research, ● Acquisition plans, ● Templates for requesting quotes, ● Identified sources of supply, and ● Independent Government Cost Estimate calculation templates.	[For internal action]	90 days
39	Acquisition Tiger Team	Send out Request for Information (RFI) or conduct other market research activities to find qualified small business and socio-economic concerns to leverage set aside programs and other authorities to streamline the migration acquisitions to the greatest extent possible to identify qualified 8(a) companies that are able to assist agencies with migrations to email cloud technologies.	Public release	90 days
40	OMB	Create acquisition/migration cadres, consisting of information technology and acquisition specialists that will be sent to early adopter agencies to help with license and migration acquisitions-related challenges.	[For internal action]	180 days
41	OMB, in coordination with GSA	Create a pilot new acquisition tactics for cloud email and collaboration licenses including but not limited to those discussed above and outlined in Appendix D.	[For internal action]	240 days

42	GSA	Continue to work with existing cloud email and collaboration providers, and will prioritize approval of a FISMA-High offering.	[For internal action]	None given
Shared Services to Enable Future Network Architectures Improve Existing and Provide Additional Security Shared Services				
43	DHS, in partnership with GSA	Complete the acquisition strategy for new, long-term task orders to offer CDM lifecycle support for Phases 3 and 4.	Government-wide release	60 days
44	DHS	Obtain initial ATO for CDM Group F Platform. Submit a plan to OMB that details the expectations and timelines for onboarding non-CFO Act agencies to the SSP.	[For internal action]	125 days
45	DHS	Complete the data exchanges between the agency- and Federal-level dashboards to provide enterprise-wide situational awareness of an agency's cyber posture.	OMB	150 days
46	DHS, in partnership with the Federal CIO Council	Implement a concept of operations for the Federal dashboard as well as procedures to manage cyber risks across the Federal enterprise.	[For internal action]	180 days
47	OMB, GSA, and DHS	Identify potential offerings to provide SOC as a Service capabilities to other agencies across the Federal Government.	[For internal action]	180 days
48	GSA, in coordination with OMB and DHS	Lead contracting efforts to also offer commercially available SOC as a Service capabilities to Federal agencies.	Government-wide release	180 days
49	Selected Agency/ies	Provide a pricing model in alignment with the cloud migration strategy and timeline outlined within the Report.	OMB and DHS	210 days
50	DHS	Work with SOC-as-a-Service providers to ensure that NCPS and CDM capabilities and outcomes can be achieved and that the visibility remains aggregated across cloud and on premise security capabilities.	[For internal action]	None given

Appendix G: Summary of Comments Received

More than 100 companies and individuals submitted comments during the three week public comment period for the IT Modernization Report. Overall, the comments reaffirmed the importance of modernizing Federal IT, and validated that the proposed approach is on the right track. The comments offered diverse and at times conflicting suggestions, and ranged from strategic thoughts to detailed implementation guidance.

The ATC strove to keep this report at a strategic level, and will make the more detailed 'implementation level' comments available to the teams who will drive specific modernization efforts across Federal IT. Several comments also noted the need to fundamentally reform or tweak current statutory provisions, and the ATC will provide these recommendations to existing activities which are already charged with these statutory reform areas.

All comments received are publically posted, but this appendix will highlight some of the key themes that emerged during the comment review.

Need for technical diversity and efficiency
Many comments stressed the need to future-proof the Government's systems, keep pace with innovation and future standards, maintain vendor and technology neutrality, and recognize the validity of diverse approaches to securing data, applications, networks, and services. Comments also suggested adopting modern approaches to development and operations such as DevOps and continuous delivery and automate more of the functional/security testing, integration, deployment, and operations of applications.

Accreditation and cybersecurity
Comments emphasized the benefits of leveraging FedRAMP authorization, suggested improvements to the FedRAMP process, asserted need to enforce reciprocity, suggested utilizing the native security capabilities (such as machine learning and big data analytics) offered by the cloud service providers, and potential for automating the sharing of classified threat intelligence with cleared service providers.

Network modernization and data level security
Comments emphasized the importance of network level security, advised that tools should focus on outcomes not mechanisms, that controls must be placed in closer proximity to the data, and that users, cloud APIs, and individual devices need to be considered as access control shifts from the network perimeter. Comments also emphasized that controls must be placed in closer proximity to the data, and that cloud access security brokers (CASBs) should be used to provide secure access to cloud resources.

Acquisition strategy and workforce
Several comments indicated concern over halting or pausing acquisitions in progress, the need for reform of the acquisition and budgeting processes, and observations that acquisition cycles needed to become more rapid and agile. Comments also suggested that the acquisition of modern IT requires a holistic approach (technical, cybersecurity, and contracting) supported by a trained and experienced workforce.

Shared services and the acquisition pilot
Comments suggested that the discussion and policy around shared service be clarified. Several comments mentioned that contract consolidation on EIS was essential, while others mentioned that the strategy might stifle innovation and competition. The ATC is committed to the strategy of

leveraging the competitively awarded EIS contract to assist with consolidation efforts. Comments suggested that the acquisition pilot would be useful in proving out the Government's objectives, while others suggested it too narrowly scoped. Comments also recommended that specific vendor names be removed from the notional examples in the appendix.

Examples of key points derived from the comments is included in the section below.

Question 1 - What are major attributes that are missing from the targeted vision? (Appendix A, Appendix B)

Comments, in response to this question suggested the report should:

(i) make clear the section only described some of the approaches to be used;
(ii) include the concept of logical vice physical separation of data;
(iii) consider including multi-factor authentication;
(iv) consider including the concept of least privilege;
(v) consider expanding the discussion regarding software lifecycle automation and security testing.

Many of the comments confirmed that the attributes were on the right track or offered additional suggestions and insights to attributes proffered within the report.

Question 2 - What are major attributes that should not be included in the targeted vision?

Comments, in response to this question, suggested the report should:

(i) remove references to specific companies;
(ii) remove or revise the suggestion that agencies halt procurement actions that are underway;
(iii) expand the description and approaches to cybersecurity assessment and authorization.

Many of the comments confirmed that the attributes were on the right track or offered additional suggestions and insights to attributes proffered within the report.

Question 3 - Are there any missing or extraneous tasks in the plan for implementing network modernization & consolidation?

Question 4 - Are there any missing or extraneous tasks in the plan for implementing shared services to enable future network architectures?

Comments and recommendations in response to questions 3 and 4 were similar and suggested or implied that the report:

(i) should clarify the definition, description, and/or purpose of employing shared services;
(ii) should identify and address obstacles to adopting shared services or network consolidation;
(iii) should, relative to item (ii) recommend that a greater focus and actions be placed on addressing issues relative to the FAR;
(iv) should acknowledge need to reuse existing accreditation packages (aka foster reciprocity among agencies);
(v) relative to item (iv) above, should suggest an activity to improve reciprocity and identify capabilities to automate NIST RMF Framework;
(vi) reinforce the need for training and career development for professionals involved in accomplishing the goals articulated in the report.

Many of the comments confirmed that the tasks were appropriate and/or offered additional enhancement to the identified tasks.

Question 5 What is the feasibility of the proposed acquisition pilot? (Appendix D)

Comments, in response to this question, suggested that the report:

(i) should clarify the intent, purpose, scope, expected outcomes, and assessment criteria of-and-for the pilot;
(ii) should consider expanding the pilot to other shared services;
(iii) should de-identify service providers and include contracting options.

The comments generally confirmed that a pilot was a valid idea and offered additional suggestions, approaches, and identified potential pit-falls.

We want to express appreciation for the sincerity, depth of thought, and time taken by each of the commenters and encourage the community to go to the public website and read each of the submissions.