Cybersecurity

> Our cybersecurity goal is simple: To support an Open and Transparent Government where the People's Information is protected and Privacy, Civil Rights, and Civil Liberties are preserved.
>
> — Gen. Gregory Touhill, U.S. Chief Information Security Officer, Office of Management and Budget

Summary

Cost	The proposed FY 2017 President's Budget requests $19 billion for cybersecurity, a 35 percent increase over FY 2016 funding levels. Sustained public attention and funding is needed to make progress in this key policy area.
Accountability	A number of Chief Information Officers (CIOs) said they often do not have the flexibility to quickly incorporate safeguards to address newly-discovered vulnerabilities due to lengthy and complex Federal procurement and hiring processes and competing priorities.
Risk	High-profile incidents such as the Office of Personnel Management (OPM) data breaches highlighted the vulnerability of the government's IT systems and prompted greater attention on Federal cybersecurity initiatives and progress.
Policy	Recently, Federal cybersecurity efforts have shifted from compliance-oriented, documentation-driven processes to continuous, automated tools and processes. Federal cybersecurity efforts span six key areas: managing cybersecurity throughout the enterprise; understanding data assets and threats, building the Federal cyber workforce and budget processes; promoting the use of standardized, centralized IT; securing the network; and securing authentication and authorization.

Cybersecurity

Overview

What is Cybersecurity?

Cybersecurity is often used interchangeably with the term "information security" and is defined by the Office of Management and Budget (OMB) as the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information;
- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; and
- Availability, which means ensuring timely and reliable access to and use of information.[1]

Federal initiatives and performance metrics related to cybersecurity have evolved over time to focus on six key areas:

1. *Managing Cybersecurity Throughout the Enterprise:* Efforts to improve how agencies budget for, plan for, and implement and oversee cybersecurity related activities throughout the agency enterprise. This includes government-wide reporting and oversight initiatives such as agency reporting on Federal Information Security Modernization Act (FISMA) implementation, CyberStat Reviews, and the President's Management Council (PMC) Cybersecurity Assessment.

Transition to IPv6

The transition from IPv4 to a more modern IPv6 does more than just enable an expansion of internet devices due to the exhaustion of IPv4 addresses, it can enable agencies to improve their cybersecurity posture. Specifically, native, end-to-end IPv6 environments enable cybersecurity staff to have an unobstructed view of network infrastructure directly supporting both the Cybersecurity National Action Plan "Secure by Design" approach and the DHS Continuous Diagnostic Mitigation (CDM) initiative. The Federal CIO and CISO should continue emphasizing agencies implement IPv6 to ensure business continuity, strategically decommission the legacy IPv4 protocol to remove this attack vector from their infrastructure, and enable secure innovations such as the Internet of Things.

2. *Understanding Data Assets and Threats:* The prioritized identification and protection of high value information and systems. High Value Assets (HVAs) are government systems, facilities, data, and aggregate datasets that may be of particular interest to potential adversaries. These assets may contain sensitive controls, instructions, or other information that is critical to national security or operational functionality.[2]
3. *Building Federal Access to Cybersecurity Talent:* A series of actions to identify, recruit, develop, retain, and expand the cybersecurity skill set of the Federal workforce, while recognizing that contractors also play vital roles in Federal cybersecurity.
4. *Promoting the Use of Standardized, Centralized IT:* The federated IT management approach that is prevalent across the Federal government today presents challenges to improving cybersecurity and delivering IT capabilities in an efficient, cost effective manner. Under this model, all agencies, regardless of size or mission, are responsible for maintaining their IT and information security resources, and many organizations struggle to maintain adequate capabilities. This problem necessitates both a further consolidation of the Federal government IT footprint and an expansion of shared, centralized services to better leverage Federal buying power, standardize IT capabilities, and realize economies of scale from aggregating data. Government-wide shared services can augment or supplement existing agency services, while providing new services for agencies without existing capabilities. For example, both the Continuous Diagnostics and Mitigation (CDM) Program Tools and the Continuous Monitoring as a Service (CMaaS) Blanket Purchase Agreement (BPA) provide a consistent set of government-wide asset, identity, and event management tools that can provide capabilities and data needed to strengthen the security posture of agency networks.[3]

Key Stakeholders

- White House Cybersecurity Coordinator
- Office of the Federal Chief Information Officer (OFCIO)
- Federal Chief Information Security Officer (FCISO)
- Office of Management and Budget, Cyber and National Security Unit (OMB Cyber)
- The President's Management Council (PMC)
- Federal CIO Council
- Federal Chief Information Security Officer Council
- National Security Council (NSC)
- Office of the Director of National Intelligence (ODNI)
- Department of Commerce, National Institute of Standards and Technology (NIST)
- Department of Homeland Security (DHS)
- General Services Administration

5. *Securing the Network:* Modernization of the Federal government's IT infrastructure through upgrades to insecure and inefficient systems, data center consolidation, and transition to cloud services, offers a path to a more efficient and secure IT portfolio. Cloud-based solutions, for instance, offer convenient, on-demand network access to a shared pool of IT resources that can be rapidly provisioned. However, while cloud-based services offer many benefits for Federal computing, they have also raised important questions about the protection of data in this new environment. Efforts like the Federal Risk and Authorization Management Program (FedRAMP), can help agencies leverage the promise of cloud by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud services. FedRAMP and other government-wide efforts to provide common capabilities to secure Federal networks, such as CDM and EINSTEIN, allow CIOs to focus on building new applications and services with the confidence that the network and infrastructure are appropriately secure.
6. *Securing Authentication and Authorization – Identity, Credential, and Access Management (ICAM):* Securing information systems and networks by better understanding and controlling which users access which resources and the rights of those users. This includes efforts to strengthen identity, credential, and access management, secure mobile devices and remote access, address insider threats, prevent data loss, and manage user permissions.

Background

Cybersecurity has taken on greater importance in recent years, driven by the continuing efforts to replace legacy government services with electronic and digital services and the rapid growth in the sensitivity, size, and variety of information held in the government's databases that support those services. Several high-profile incidents have highlighted the need to address longstanding vulnerabilities in Federal IT systems. Most notably, the 2015 breach at the Office of Personnel Management (OPM) involving the compromise of personally identifiable information (PII) and security clearance background details put approximately 21.5 million Federal employees at risk of identity theft.[4]

The early cornerstone of today's Federal cybersecurity efforts is the *Federal Information Security Management Act (FISMA) of 2002*. Congress enacted this law to improve the effectiveness of security controls for Federal information systems and to ensure adequate oversight of such activities. FISMA identified the role agencies, OMB, DHS, and the National Institute of Standards and Technology (NIST) play in government-wide efforts.[5] In 2014, Congress updated this law in the *Federal Information Security Modernization Act of 2014*.

Since 2009, a number of policy initiatives were undertaken to improve the government's cybersecurity posture. The most notable of these are the:

- 2009 Cyberspace Policy Review (60-day Review),
- 2015 Cybersecurity Sprint (Cyber Sprint),
- 2015 Cybersecurity Strategy and Implementation Plan (CSIP), and
- 2016 Cybersecurity National Action Plan (CNAP).

Cybersecurity is much more than just a technology fix—rather it is a risk management issue. When we focus exclusively on the technology we sometimes miss the real goal, which is managing the risk to the confidentiality, integrity and availability of the information the technology supports.

- Gen. Gregory Touhill,
U.S. Chief Information Security Officer,
Office of Management and Budget.

Cyberspace Policy Review (60-day Review) and Resulting Actions. In 2009, the new Administration conducted a 60-day Review of cybersecurity policies and structures inside and outside of the Federal government. The Review's findings were published in a May 2009 report to the President,[6] and include a number of recommendations which the White House implemented:[7] appointing a White House Cybersecurity Coordinator in the National Security Council, establishing a Cybersecurity Cross-Agency Priority (CAP) Goal[8] as a part of the President's Management Agenda, defining performance metrics for cybersecurity, establishing a mechanism for holding agencies accountable for their performance through OMB's CyberStat Review process,[9] and announcing other related national cybersecurity documents, strategies, and plans.[10]

30-day Cybersecurity Sprint and CSIP. While strengthening the cybersecurity of Federal networks, systems, and data continued to be an important challenge post-2009, agencies often struggled to ensure cybersecurity was resourced and prioritized on par with program delivery. The OPM cybersecurity breach in 2015 sharply refocused the attention of agency heads on the criticality of supporting CIO and Chief Information Security Officer (CISO) function within their agencies.

Capitalizing on this spotlight, OMB initiated a Cybersecurity Sprint. This effort identified a set of critical actions for Federal agencies to take within 30 days[11] and established a Sprint Team to lead an intensive review of the Federal government's cybersecurity policies, procedures, and practices.[12] The recommendations resulting from the Sprint Team's review led to an October 2015 OMB memorandum titled "Cybersecurity Strategy and Implementation Plan" (CSIP).[13] This plan:

- Reiterates agencies' responsibilities for a number of ongoing cybersecurity initiatives;
- Assigns new actions, such as agencies must identify their high value assets (HVAs) and critical system architecture, and designate a "security operations center" at each agency;
- Requires new plans and documents, such as an OMB cybersecurity shared services plan, an Improving the Security of Consumer Financial Transactions Implementation Plan, and new NIST guidance on how to recover from incidents;
- Extends actions emphasized during the Cybersecurity Sprint, such as tightening privileged user policies, practices, and procedures and addressing critical vulnerabilities identified through scanning within 30 days; and
- Designates the PMC to oversee the implementation of the CSIP, in an effort to ensure agency leadership stayed engaged in supporting CIO and CISO functions within their organizations.

CNAP and FY 2017 President's Budget. Building on the CSIP, in 2016, the White House published a fact sheet announcing a set of near-term actions to improve cybersecurity, and pave the way for a longer-term strategy to enhance cybersecurity awareness and protections. The Cybersecurity National Action Plan (CNAP):[14]

- Establishes the Commission on Enhancing National Cybersecurity;
- Creates the Federal Chief Information Security Officer (FCISO);
- Proposes the Information Technology Modernization Fund (ITMF);
- Commits to work with industry to encourage multi-factor authentication throughout public-facing Internet services and to release a new action plan for government use of multi-factor authentication;
- Highlights a number of new initiatives with expanded funding in the FY 2017 President's Budget, including a focus on expanding the cybersecurity workforce by enhancing student loan forgiveness programs for cybersecurity experts joining the Federal workforce and catalyzing investment in cybersecurity education as part of a robust computer science curriculum through the President's Computer Science for All Initiative;[15]
- Highlights new and continued privacy and security initiatives, such as the 2014 BuySecure Initiative and the re-launch of IdentityTheft.gov, together designed to protect Americans from credit card fraud and identity theft; and
- Highlights new and continued initiatives to "enhance critical infrastructure security and resilience," such as establishing a National Center for Cybersecurity Resilience, developing the Cybersecurity Assurance Program to improve the security of "internet of things" devices, and doubling the number of Department of Homeland Security (DHS) cybersecurity advisors available to assist private sector organizations involved in critical infrastructure.

The FY 2017 Budget proposes more than $19 billion for Federal cybersecurity efforts.[16] A 35 percent increase over the funding level of 2016, these resources are intended to help agencies improve their cybersecurity posture, help private sector organizations and individuals better protect themselves, disrupt and deter adversary activity, and respond more effectively to incidents. Many of the initiatives described in the CNAP would use this expanded funding.

The CNAP also established a new cybersecurity leadership position, Federal Chief Information Security Officer (FCISO). This position drives government-wide cybersecurity policy, planning, and implementation across the Federal government. In addition, the CNAP directed implementation of the first-ever Federal Cybersecurity Workforce Strategy[17] to identify, recruit, develop, and retain talent for Federal service, and proposed an IT Modernization Fund (ITMF) to provide $3.1 billion in dedicated funding to encourage agencies to replace or otherwise modernize critical systems and equipment.

Initiatives spearheaded by the Federal CIO under the direction of the White House and the PMC, such as the Cyber Sprint, have yielded positive results. A sustained focus from the highest-ranking officials in government can serve to drive the cyber risk management process, leading to better-protected Federal data and information systems. Additionally, revisiting the role and relationship of agency CISOs to program leaders and other senior management leaders such as CFOs could help ensure that agencies are setup to integrate information security concepts, practices, and initiatives throughout agency decisions at a senior level.

Current State of Key Initiatives

Managing Cybersecurity Throughout the Enterprise

Guides how agencies budget for, plan for, and oversee cybersecurity. Includes, for example, CyberStat Reviews, FISMA reporting, Cybersecurity CAP Goal Performance Updates, and PMC reporting and oversight.

Understanding Data Assets and Threats

Requires agencies to identify and protect high value information and systems that may be of particular interest to potential adversaries.

Building the Federal Cyber Workforce

Directs a series of actions to identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service.

Promoting the Use of Standardized, Centralized IT

Provides common services available to all agencies to consistently and cost-effectively implement aspects of cybersecurity initiatives, such as CDM, the CMaaS BPA, and EINSTEIN.

Securing the Network

Improves the security of external and internal infrastructure and network options for agencies. Includes initiatives to secure both external providers' networks, such as FedRAMP, and internal Federal networks, such as TIC.

Securing Authentication and Authorization – Identity, Credential, and Access Mgmt.

Provides a variety of initiatives to improve logical and physical security across agencies, including but not limited to the issuance and use of Personal Identity Verification (PIV) cards.

The themes consist of numerous efforts and actions which took place over a broad period of years, and many are ongoing today. As such, specific years are not included.

Managing Cybersecurity Throughout the Enterprise

Overall government-wide reporting and oversight initiatives help ensure a common management approach to implementing cybersecurity capabilities across the Federal government. In early 2016, the White House created a new cybersecurity leadership position, the FCISO. Established in the CNAP, this position is responsible for driving government-wide cybersecurity policy, planning, and implementation across the Federal government. The initiatives listed below are all led by the Federal CISO:

- *Annual FISMA Reporting.* Common processes that originated in FISMA and are defined by NIST[18] publications include regular reporting on a standard set of cybersecurity capabilities by Federal agencies, an annual FISMA report from OMB to Congress summarizing performance metrics from all the agencies, the categorization of systems by risk level (these guidelines are typically referred to as "FISMA High," "FISMA Moderate," and "FISMA Low")[19] and the procedures by which an agency authorizes the operation of a system in its environment. [20]

  After twelve years, an amendment to FISMA was signed into law – the Federal Information Security Modernization Act of 2014. This update provides several modifications, such as clarifying OMB's government-wide cybersecurity oversight role and DHS's responsibility to administer the implementation of cybersecurity policies and practices by Federal agencies (the original FISMA had been passed before DHS was established). FISMA 2014 also led to OMB issuing the first revision of Circular A-130 "Management of Information as a Strategic Resource" since 2000. [21]

- *CyberStat Reviews.* CyberStat Reviews are deep-dive, evidence-based, face-to-face engagements with Federal CIOs and CISOs, built around comprehensive reviews of agency-specific cybersecurity postures and select government-wide cybersecurity programs. Through these targeted, high-level engagements, OMB and agency leaders are able to frankly discuss persistent cybersecurity concerns and collaborate to make sure challenges are adequately addressed and resourced. The number conducted per year increased from eight in FY 2014 to 24 in FY 2016. Reviews in FY 2016 focused on information security governance, strong authentication, and agency protections of HVAs. In general, OMB leverages the CyberStat process to uncover best practices and common challenges across the Federal enterprise in areas such as CDM implementation, rationalization of the TIC and cloud policies, and common needs for cybersecurity workforce and training. OMB's CyberStat Review process was established in January 2011[22] and updated in 2015.[23]
- *PMC Cybersecurity Assessment.* Since 2015, OMB has conducted quarterly engagements with agencies regarding their progress implementing Federal policies and priorities. The executive visibility gained by using the PMC to connect the Federal CIO with Deputy Secretaries is a critical factor in improving the state of Government-wide cybersecurity. PMC members discuss the status of their cybersecurity efforts and recommendations for improving performance using a maturity model based on the five function areas of the NIST Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover. These updates can factor into OMB's cybersecurity budgeting process, where agency performance in specific function areas can be matched to both previous and projected spending to identify opportunities for investments to support critical capabilities.

Understanding Data Assets and Threats

Agencies' efforts to identify, prioritize, and protect their most sensitive assets and data are a major component of government-wide cybersecurity. These assets may contain sensitive controls, instructions, or other information that is critical to national security or operational functionality.

- *High Value Assets.* In 2015, OMB published the Federal Information Security and Privacy Management Requirements to identify and assess security risk around HVAs and to align current processes with the NIST Cybersecurity Framework.[24] However, agencies struggled to settle on a common definition for HVAs. OMB brought agency CIOs together to agree upon a common understanding of policies to identify, manage, and protect HVAs. OMB was then able to apply these policies in subsequent guidance, such as the CSIP,[25] and further codify them in the CNAP. OMB plans to take further steps to formalize these approaches through additional memoranda in FY 2017.

Building the Federal Cyber Workforce

The Federal Cybersecurity Workforce Strategy, released in 2016, focuses on improving how agencies identify, recruit, develop, retain, and expand the pipeline of the best, brightest, and most diverse cybersecurity talent for Federal service.[26] It identifies actions for OPM, the National Initiative for Cybersecurity Education (NICE), and other Federal agencies to improve cybersecurity workforce planning.

The Strategy establishes four key initiatives:

- *Identify Cybersecurity Workforce Needs.* Seeks to improve the government-wide understanding of cybersecurity workforce needs by identifying key capability and capacity gaps in order to enhance workforce planning;
- *Expand the Cybersecurity Workforce through Education and Training.* Entails working with educational institutions, professional organizations, training organizations, and other experts on cybersecurity program guidance from P-12 through university-level education to significantly expand the pipeline of skilled cybersecurity talent;
- *Recruit and Hire Highly Skilled Talent.* Establishes government-wide and agency-specific efforts to expand the cybersecurity workforce through recruitment of highly skilled talent. Streamlines the hiring and security clearance process while still meeting applicable law and standards; and
- *Retain and Develop Highly Skilled Talent.* Promotes an enterprise-wide approach to retention and development to support the continued enhancement of the Federal cybersecurity workforce.

Promoting the Use of Standardized, Centralized IT

The federated nature of agencies' IT management – distributing responsibilities across many agencies, bureaus, and programs – can be a significant impediment to improving cybersecurity. Under this model, all agencies, regardless of size or mission, are responsible for maintaining their own IT, and many organizations struggle to maintain adequate security capabilities.

One approach to addressing this disparity is to develop common, centrally-managed services to better leverage Federal buying power, cybersecurity skillsets, and standardize security capabilities. These efforts help agencies better secure their own networks and accelerate their access to secure external solutions. For example, both the CDM Program Tools and the CMaaS BPA provide government-wide capabilities that enable Federal agencies to strengthen agency networks.[27] The goal of the CDM program is to bring consistency to the security capabilities used by agencies for basic cyber hygiene functions, while also procuring these tools in a cost effective manner. Similarly, DHS's EINSTEIN program was designed to protect agencies' unclassified networks through shared situational awareness across the government, as threats detected at one agency are shared with all others.

Other efforts to ensure agencies have access to modern systems and services include taking steps to centralize IT for small agencies, using a Small Agency Network as a proof of concept. Other potential areas for greater centralization and standardization include: mobile security services, network segmentation services, identity, authentication, and authorization services, digital rights management, and encryption services.

- *Continuous Diagnostics and Mitigation (CDM) program*. CDM enhances the government's ability to collect and act on automated information regarding Federal IT assets. The first phase of CDM, currently being deployed, allows agencies to identify assets on a continuous basis. CDM also allows for information to be fed to a Federal-level dashboard, which provides government-wide visibility into the current state of Federal assets. Phases 2 and 3 will extend the visibility of these tools into additional aspects of Federal assets, users, devices, and intrusions.[28] Agencies are in the process of deploying to their own dashboards but have not yet connected to the Federal dashboard.
- *EINSTEIN*. The DHS National Cybersecurity Protection System, commonly known as EINSTEIN, offers a consistent suite of tools for network boundary protection to agencies. All major Federal agencies have adopted the intrusion detection services of EINSTEIN. The next phase of services offers a capability to disable attempted intrusions before harm is done, which would address approximately 85% of the cybersecurity threats affecting Federal civilian networks. As a shared service, EINSTEIN has encountered some resistance from agencies seeking to retain greater control over their tools, delaying full deployment.

Securing the Network

Modernization of the Federal government's IT infrastructure, such as through upgrades to insecure and inefficient systems, data center consolidation, and transition to cloud services, offers a path to a more efficient and secure IT portfolio. Greater agency interest in cloud-based solutions has raised important questions about the protection of data in this new environment. Several key initiatives are currently underway to transition Federal agencies to more secure and efficient platforms which would allow CIOs to focus on building new applications and services with the confidence that the network and infrastructure are appropriately secure.

- *IT Modernization Fund.* Of the $82 billion in Federal IT spending planned for 2017, approximately 78 percent ($63 billion) is dedicated to maintaining legacy IT investments. These systems may pose security risks, such as the inability to utilize current security best practices, including data encryption and multi-factor authentication, as well as operational risks, such as rising costs and inability to meet mission requirements.

  To help address these challenges, the President proposed the creation of a $3.1 billion Information Technology Modernization Fund (ITMF) as part of the FY 2017 President's Budget and the Cybersecurity National Action Plan (CNAP). Federal agencies would use this revolving fund at GSA "to retire, replace or upgrade hard-to-secure legacy IT systems and transition to new, more secure, efficient, modern IT systems, while also establishing long-term mechanisms for Federal agencies to regularly refresh their networks and systems based on up-to-date technologies and best practices."[29] Envisioned as a revolving fund which agencies would reimburse based on the cost savings they achieve by replacing legacy IT systems with more efficient alternatives, the ITMF is intended to enable not only improvements to agencies' cybersecurity posture, but also to lead agencies to a modernized IT infrastructure which supports modern digital services.

- *Secure Cloud Adoption.* Cloud-based solutions offer convenient, on-demand network access to a shared pool of IT resources that can be rapidly provisioned. This allows agencies to get out of the business of managing the full stack of IT services themselves and to avoid overhead costs by paying only for those resources they use.

  To help realize the benefits of cloud computing, OMB issued the Federal Cloud Computing Strategy in 2011. The strategy encouraged agencies to use cloud-based services in order to improve resource utilization, increase service responsiveness, and accrue meaningful benefits in efficiency, agility, and innovation. While cloud-based services offer many benefits for Federal computing, they have also raised important questions about the protection of data in this new environment. For this reason, in 2011, OMB established the Federal Risk and Authorization Management Program (FedRAMP).[30] The program provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud services in order to allow cloud service providers to achieve a single authorization for a given service that may then be used by other agencies to establish their own authorizations, providing efficiencies, cost savings, and a common security baseline. FedRAMP includes a Joint Authorization Board (JAB) composed of the CIOs of the Department of Homeland Security (DHS), Department of Defense (DOD), and the General Services Administration (GSA), and is operated by a GSA-based Program Management Office (PMO).

  As agencies adopt cloud services, they have begun to experience difficulties complying with the Trusted Internet Connection (TIC) initiative, which lays out an architecture for consolidating and protecting agency connections to the public internet in order to ensure these connections are secure. Since its initiation in 2008, the government has reduced the number of Federal connections to the Internet from several thousand to 65 in 2015, and has helped provide a secure internal network infrastructure for CIOs to access. However, because TIC relies on a centralized access point (while cloud is based on a decentralized model), complying with both policies has created problems for agencies and industry alike. Given the growing importance of protecting Federal data whether hosted in a cloud, a data center, or traversing the internet, OMB has launched an effort to align existing policies related to TIC and cloud service adoption.

- *Continuous Diagnostics and Mitigation (CDM).* A key component of this effort is CDM, which continues to be a Federal priority in making real-time data on an agency's risk posture available to decision makers.[31] CDM assists agencies in maintaining continuous awareness of prioritized risks and security vulnerabilities at an enterprise level. While this program is a part of the effort to establish standardized, centralized IT for CIOs to build off of, it is also a basic component of identifying gaps in securing the network. By improving agency awareness of what is running on their networks, CDM makes it easier to target patch updates and address software vulnerabilities that may be weakening the resilience of the network.

Securing Authentication and Authorization — Identity Credential and Access Management

A number of efforts focus on better understanding and controlling which users access which resources. These include efforts in Federal Public Key Infrastructure (PKI), Federal Identity, Credential, and Access Management (FICAM), securing mobile devices, improving citizen authentication to government and private sector services, as well as broader strategies to narrowly define privileged user permissions. An overall summary of the FICAM topic area can be found at IDManagement.gov.

- *PIV Cards and HSPD-12*. One of the recommendations from the 9/11 Commission Report from 2004 was to ensure that only appropriate people are accessing Federal facilities ("physical access") and IT systems ("logical access").[32] Many cybersecurity threats gain unauthorized access to a system and its data by falsely claiming to be a user who has those privileges or access. Ensuring that someone is who they say they are and that only authorized people have access to the appropriate Federal facilities and systems became a major initiative in Federal cybersecurity efforts, beginning with the release of "Policies for a Common Identification Standard for Federal Employees and Contractors," more commonly known as "HSPD-12."[33] This set in motion a series of actions to develop a PIV card and to work with all agencies to issue the PIV card to employees, contractors, and others who require its use for physical and logical access, and to increase interoperability between agencies.
- *National Strategy for Trusted Identities in Cyberspace (NSTIC) and other efforts*. Recognizing that Federal leadership could also play a role in strengthening identity verification and transactions outside of government, Commerce published the NSTIC in April 2011. This established the NSTIC program at Commerce to coordinate the Federal government and private sector to "increase adoption of trusted digital identity solutions" inside and outside of government.[34] Relatedly, the MyUSA and Connect.gov initiatives were also launched to expand government online citizen-facing services' ability to accept credentials issued from other providers, such as Google accounts or State drivers' licenses. In 2016, GSA consolidated these efforts into a new initiative led by 18F with similar goals called Login.gov.[35]

.

Metrics and Oversight

Primary Objective Emphasized in Metrics and Oversight

Government-wide reporting for cybersecurity focuses on agency progress implementing key government-wide initiatives to address critical vulnerabilities, identify emerging threats and vulnerabilities, and evaluate agency responses to incidents.

Examples

The primary data collection for cybersecurity is that collected under FISMA each year (largely submitted through the DHS Cyberscope data collection tool). The data collected under FISMA each year can be varied and extensive, with one agency describing the requirement as "120 metrics quarterly." OMB has made efforts to pare down the reporting over time, but the requirements are still significant. OMB strives to use the concept of "report once, use many times," leveraging the FISMA data to inform PortfolioStats, CyberStat Reviews, the PMC Cybersecurity Assessment, and Cybersecurity CAP goal reporting. Additionally, OMB analyzes agencies' HVA submissions, data collected by DHS under its "binding operational directive" activities, US-CERT incident reporting data, and data provided by the FedRAMP Program Management Office.

While cybersecurity-related KPIs have been included in PortfolioStat for every year of its operation, cybersecurity oversight is conducted in greater depth through the PMC Cybersecurity Assessments, and CyberStat Reviews. Additionally, the Cybersecurity CAP Goal reports progress on implementing priority cybersecurity capabilities publicly. The PMC Cybersecurity Assessments are quarterly and include Deputy Secretaries of major Federal agencies and the Federal CIO. The CyberStat Reviews currently assess 2-4 agencies per month, and include DHS and NSC leaders as well as OMB officials.

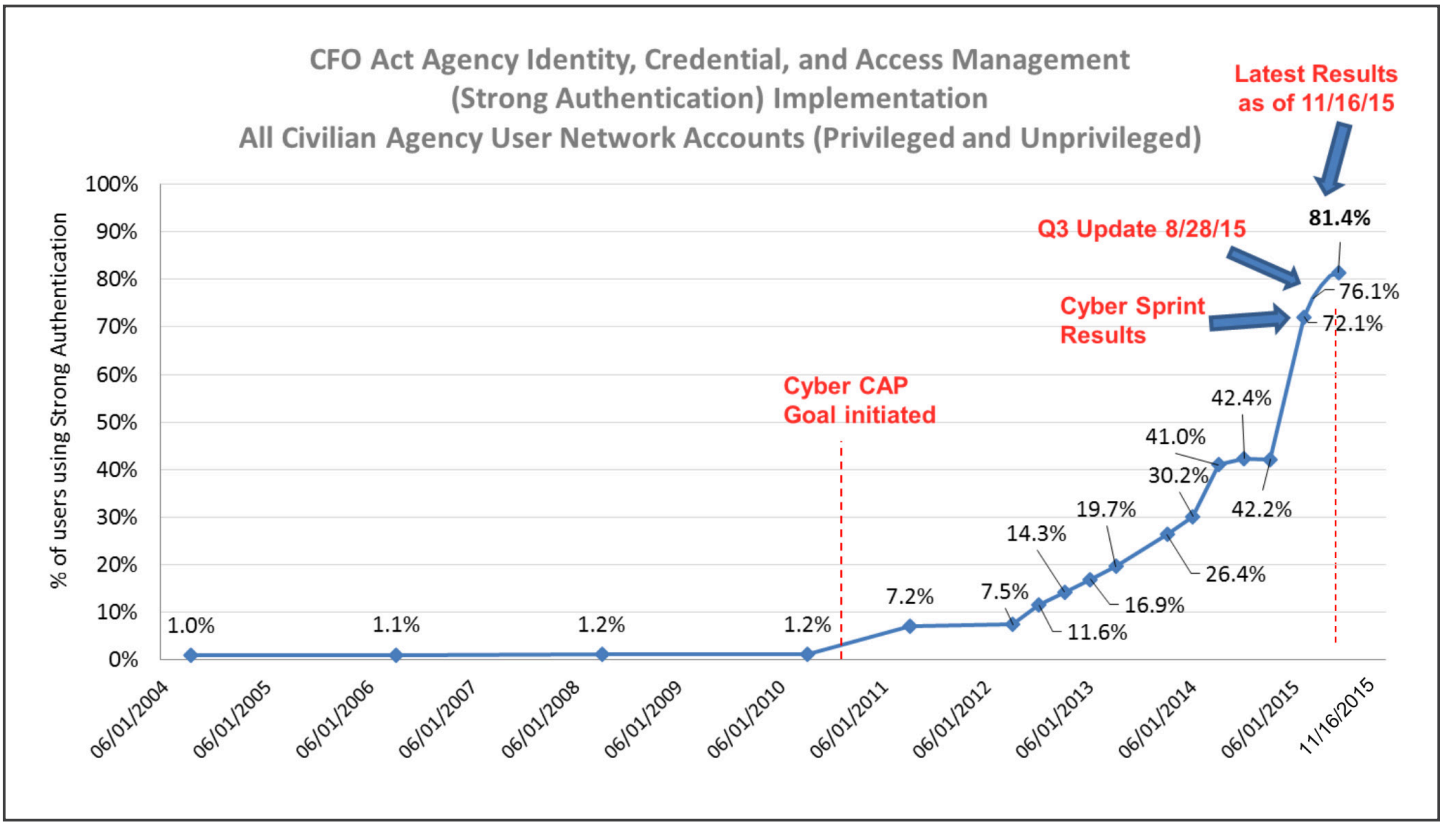
Lessons Learned

Continued efforts to remove less valuable metrics and survey questions from FISMA have made progress year to year, though new vulnerabilities, initiatives, and threats have applied continued pressure to expand the reporting requirements.

One of the successful aspects of the Cyber Sprint was its focus on a small number of actions, allowing leadership to focus on a compact set of priorities rather than the large number of FISMA metrics, which represent diverse requirements. A key opportunity, therefore, is to explore more efficient oversight methods which help agencies and others focus on the most relevant aspects of this complex topic.

The Cyber Sprint rapidly improved agencies' implementation of the HSPD-12 initiative and is a model for future oversight. HSPD-12 required agencies to use two-factor authentication for physical and logical access by 2008.[36] However, PIV card issuance historically lagged behind targets and was inconsistent across agencies.[37] In fact, many agencies continued to require PIV cards for network access at or below a rate of just 1% for their civilian network accounts through 2010.[38] As indicated in the figure below, government-wide PIV compliance increased from 42 percent to 72 percent as a result of this concerted leadership attention.[39] This was a major success, and has been cited by many agency CIOs as a key example of effective policy implementation and oversight from OMB.

Figure E1: PIV Compliance Sprint Results, 2015 Q4 Update[40]



Overall Findings

This sections presents key findings based on review of policy documents, CIO interviews, and analysis of OMB key metrics and oversight over the years. These findings are focused on government-wide activities rather than the circumstances in any particular agency.

FINDING #1

Government Procurement Processes Lack the Flexibility to Adapt to Evolving Cyber Threats.

A number of CIOs stated that the Federal procurement process is lengthy and complex, and does not provide them with the flexibility needed to respond quickly to cybersecurity threats. New cybersecurity vulnerabilities are discovered every day, and the tools required to mitigate those vulnerabilities may change just as quickly. The current Federal procurement process cannot adapt at that pace, leaving agencies with limited options in defending themselves against emerging cyber threats. With potential adversaries operating with access to the newest technologies, and focusing more of their efforts on compromising government systems, agencies need to be timely and flexible in their defenses. If a new vulnerability is discovered in an existing vendor's system, the agency's contract agreement may make it difficult for agencies to switch to a different provider. The ability to respond to newly-discovered vulnerabilities in a more agile manner could improve the ability of agencies to respond to evolving threats. Agencies can also benefit from the additional testing and patching of software-based vulnerabilities that can come from open public review of Federal source code.[41] Efforts to address broader challenges in the IT acquisition and contracts area could improve the agility of agencies' to respond to cybersecurity threats or address vulnerabilities.[42] For example, GSA is adding a set of Highly Adaptive Cybersecurity Services (HACS) Special Item Numbers (SINs) to IT Schedule 70 "to better enable GSA to provide agencies quick, reliable access to key cybersecurity services before, during, and after cyber threats occur."[43]

It sometimes takes too long to procure things especially when it comes to Cyber. A year to procure, 4 months to install and implement, too long to address the issue.

- Agency CIO

FINDING #2

The Federal IT Workforce Must Be Expanded and Strengthened in Order to Adequately Address Challenges in Cybersecurity.

The Cyber Sprint highlighted the need to improve recruitment, retention, and training for the Federal IT workforce at large and, in particular, the Federal cybersecurity workforce. For example, many CIOs explained that they had identified well-qualified candidates for cybersecurity positions, but those candidates ended up taking other jobs—often in the private sector. CIOs attributed this to multiple issues with the Federal hiring environment: the process takes too long, relies on a confusing website/application procedure, and agencies cannot offer competitive salaries. For example, the hiring process for Federal agencies often takes significantly longer than that in the private sector and requires candidates to navigate the USAJobs process, which can be more difficult than applying for a private sector job. Even if a candidate does go through the whole process, HR selection officials with limited cybersecurity subject matter expertise may misevaluate candidates' capabilities, leading to under-qualified candidates advancing ahead of well-qualified ones.

Moreover, CIOs repeatedly mentioned that it is difficult for agencies to offer well-qualified candidates a salary that is competitive with the private sector. This salary issue also creates problems in retaining talented government employees. Internal reviews by OMB have identified additional potential issues, such as job candidates' concern that a private sector position may give them more autonomy and a more flexible work culture than a Federal information security position.

Finally, Federal hiring practices frequently rely on traditional career development models. However, many of today's information security professionals may take non-traditional career paths less focused on obtaining secondary education degrees, making it difficult for Federal hiring strategies to identify them.

Despite government-wide initiatives such as the cyber direct hire authority, some CIOs related concerns that the Cybersecurity Workforce Strategy focuses too heavily on long term solutions rather than helping CIOs with their immediate needs. However, other policy ideas being explored by OMB may address these issues, such as having OPM organize a cybersecurity recruitment fair for all Federal agencies that showcases hiring authorities and new cybersecurity career paths.

Facing significant obstacles to hiring new cybersecurity workforce, agencies have invested in training to improve the cybersecurity subject matter expertise of existing IT staff. Recent investments in workforce training have been implemented around cybersecurity concepts such as phishing and malware, including agency-wide trainings for non-experts, and expert-focused enrichment opportunities like the course on malware reverse engineering offered through US-CERT.[44] Similar Federal training programs and courses have augmented the adoption of modern automated practices such as CDM and tools like EINSTEIN.

FINDING #3

Cybersecurity Sprint Demonstrated a Highly-Effective Model of OMB-to-Agency Policy Formulation and Implementation.

The Cyber Sprint was praised by most CIOs as a success in accomplishing its goals, and provided a valuable set of lessons learned in how OMB and the White House could involve agencies in a collaborative effort. CIOs suggested that the Cyber Sprint was successful due to two key factors: ongoing involvement by high-level White House and OMB leadership, as well as early collaboration between government-wide policy makers and agency CIOs to design implementation plans that allowed agencies the flexibility to choose an approach that worked with their specific needs. CIOs listed some lessons learned from the Cyber Sprint: the need for continuous engagement between OMB and agency leadership and between agency leadership and CIOs; providing agencies with verifiable and achievable objectives and timeframes; allowing agencies some latitude within a policy framework to execute strategies that work within their structural constraints, and obtaining agency buy-in prior to the start of a new policy initiative.

Another factor cited for the Cyber Sprint's success was that it asked agencies to focus on a small number of actions. This is compared to the broader, high number of FISMA metrics — many with unclear causal relationships to each other — that create a perception that "everything is important," which runs the risk of some leaders concluding "nothing is important."

The Cyber Sprint was helpful because it allowed us to focus on privileged users. The Deputy Secretary and CIO were in charge and it was very focused/scoped with a lot of follow-up.

- Agency CIO

FINDING #4

High Visibility in Cybersecurity Leads to Multiple Policy Messages, Metrics, and Priorities.

CIOs have stated that they face an increasing number of reporting requirements in relation to their cybersecurity efforts, even while OMB has tried to reduce the requirements. The required reporting used in annual FISMA reports, CAP goal reporting, PMC meetings, and West Wing reviews of cybersecurity has led to a large number of varied metrics and information, according to agencies. Although many agency CIOs agree that there is some alignment of metrics across oversight mechanisms, they still note that reporting could benefit from streamlining and centralization. Cyber-related metrics, especially those used in PortfolioStat, are some of the most consistent year-to-year of any IT policy area. Despite this consistency, agencies did not mention PortfolioStat as a major channel for cybersecurity discussions. Instead, agencies pointed to CyberStat Reviews and the PMC Assessment as the driving force for cybersecurity discussions. The proliferation of cybersecurity efforts has led to an environment where agencies seek guidance in identifying immediate priorities. While OMB and other government-wide IT leaders in cybersecurity policy have taken steps to reduce the variety and burden of these reporting requirements, continued efforts to better align agency attention with the highest impact actions could be valuable.

300% more metrics (120 metrics quarterly) are being asked for us to report in regards to FISMA. Too many requirements, hard to tell what is a priority. Our challenge is to convince Tony and others [to streamline]. I only have time for 4 things and you are asking for 40.

- Agency CIO

Notes

1. Circular A-130: Managing Information as a Strategic Resource. https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

2. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

3. For more information on Continuous Diagnostics and Mitigation (CDM) Program, see: http://www.gsa.gov/portal/content/177883

4. For more information about the OPM breach, see: https://www.opm.gov/cybersecurity/cybersecurity-incidents/

5. Public Law No. 107–347. E-Government Act of 2002. 12/17/2002. https://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf

6. White House Press Release. "Cybersecurity event fact sheet and expected attendees" 5/29/2009. https://www.whitehouse.gov/the-press-office/cybersecurity-event-fact-sheet-and-expected-attendees and "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure": https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

7. White House Press Release. "Fact Sheet: The Administration's Cybersecurity Accomplishments". 5/12/2011. https://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-administrations-cybersecurity-accomplishments

8. "Cybersecurity" became one of the original "interim CAP goals" announced in 2012 in the FY 2013 President's Budget, as described in GAO report on CAP Goals. GAO-14-526. Managing For Results: OMB Should Strengthen Reviews of Cross-Agency Goals. 5/20/2014. http://www.gao.gov/assets/670/664022.pdf

9. CyberStat was established in the January 2011 OMB memorandum M-11-33 and DHS FISM 11-02 message. M-11-33. FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 9/14/2011. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf

10. Other documents include: a publicly-releasable summary of the "Comprehensive National Cybersecurity Initiative" (CNCI)--an internal guiding cybersecurity policy document, the "International Strategy for Cyberspace" (May 2011), the "National Cyber Incident Response Plan" (NCIRP), OSTP's "Cyber Research and Development Framework," and the "National Strategy for Trusted Identities in Cyberspace" (NSTIC) (April 2011)

11. Enhancing and Strengthening the Federal Government's Cybersecurity. 6/11/2015. https://www.whitehouse.gov/sites/default/files/omb/budget/fy2016/assets/fact_sheets/enhancing-strengthening-federal-government-cybersecurity.pdf

12. The Sprint Team, led by OMB was comprised of representatives from the National Security Council (NSC), the Department of Homeland Security (DHS), the Department of Defense (DOD), and other Federal civilian and defense agencies

13. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

14. White House Press Release. "Fact Sheet: Cybersecurity National Action Plan." 02/09/2016 https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

15. White House Press Release. "Fact Sheet: President Obama Announces Computer Science For All Initiative". 01/30/2016. http://www.whitehouse.gov/the-press-office/2016/01/30/fact-sheet-president-obama-announces-computer-science-all-initiative-0

16. White House Press Release. "Fact Sheet: Cybersecurity National Action Plan". 02/09/2016. https://www.whitehouse.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

17. M-16-15. Federal Cybersecurity Workforce Strategy. 06/12/2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

18. FISMA requires agencies to follow certain instructions from organizations such as OMB and NIST. For example, FISMA requires agencies to comply with NIST's Federal Information Processing Standards (FIPS) and OMB FISMA reporting requirements, which in turn reference other NIST documents called Special Publications (SPs), such as those describing how to conduct certification and accreditation procedures. See "Page iv" of NIST SP 800-37 for a summary of this framework: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

19. This requirement is described in FIPS 199. Standards for Security Categorization of Federal Information and Information Systems. 2/2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf and NIST SP 800-60. Guide for Mapping Types of Information and Information Systems to Security Categories. 8/2008. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

20. NIST SP 800-37. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. 2/2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

21. Circular A-130 Managing Federal Information as a Strategic Resource. July 2016. https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

22. M-11-33. FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. 9/14/2011. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf

23. M-16-03. Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements" 10/30/2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

24. M-16-03. Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements. 10/30/2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf

25. M-16-04. Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government. 10/30/2015. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf

26. M-16-15. Federal Cybersecurity Workforce Strategy. 6/12/16. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-15.pdf

27. For more information on Continuous Diagnostics and Mitigation (CDM) Program, see: http://www.gsa.gov/portal/content/177883

28. M-14-03. Enhancing the Security of Federal Information and Information Systems. 11/18/2013. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

29. FY2017 Budget of the United States. "Analytical Perspectives: Information Technology." Available at: https://www.whitehouse.gov/sites/default/files/omb/budget/fy2017/assets/ap_17_it.pdf

30. For more detailed information about efforts related to FedRAMP, see Policy Chapter B: IT Infrastructure Modernization. Also see: Office of Management and Budget. "Security Authorization of Information Systems in Cloud Computing Environments". 11/08/2011. https://www.fedramp.gov/files/2015/03/fedrampmemo.pdf

31. M-14-03. Enhancing the Security of Federal Information and Information Systems. 11/18/2013 https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

32. "9/11 Commission Report". 2004. https://9-11commission.gov/report/911Report.pdf

33. President George W. Bush. HSPD-12. Policy for a Common Identification Standard for Federal Employees and Contractors. 8/27/2004. http://fas.org/irp/offdocs/nspd/hspd-12.html and M-05-24. Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors. 8/5/2005. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf

34. NIST. "National Strategy for Trusted Identities in Cyberspace (NSTIC): Our Focus". https://www.nist.gov/itl/nstic/our-focus

35. 18F blog post. "Building a modern shared authentication platform". 5/10/2016. https://18f.gsa.gov/2016/05/10/building-a-modern-shared-authentication-platform/ and see Login.gov homepage: https://pages.18f.gov/identity-intro/

36. President George W. Bush. HSPD-12. Policy for a Common Identification Standard for Federal Employees and Contractors. 8/27/2004. http://fas.org/irp/offdocs/nspd/hspd-12.html

37. GAO-11-751. Personal ID Verification:Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards . 9/20/2011. http://www.gao.gov/new.items/d11751.pdf

38. Performance.gov. "Cross-Agency Priority Goal: Cybersecurity". FY 2015 Q4 Update. https://www.performance.gov/content/cybersecurity#progress-update

39. Performance.gov. "Cross-Agency Priority Goal: Cybersecurity". FY 2015 Q4 Update. https://www.performance.gov/content/cybersecurity#progress-update

40. Ibid

41. For more information about government-wide efforts to encourage public review of Federal source code, see: M-16-21. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software. 8/8/2016. https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m_16_21.pdf

42. For more information about the IT Acquisition and Contracts policy area, see Policy Chapter F: IT Acquisition and Contracts Management

43. General Services Administration. "GSA IT Schedule 70 to Incorporate Highly Adaptive Cybersecurity Services SIN". 08/17/2016. https://interact.gsa.gov/document/gsa-it-schedule-70-incorporate-highly-adaptive-cybersecurity-services-sins

44. National Initiative For Cybersecurity Careers And Studies. "Malware Reverse Engineering". 10/4/2016. https://niccs.uscert.gov/training/search/anrc/malware-reverse-engineering