Federal Cybersecurity Risk Determination Report and Action Plan

May 2018

Contents

How to Read This Report

The Office of Management and Budget (OMB) is publishing this Federal Cybersecurity Risk Determination Report and Action Plan (Risk Report) in accordance with Presidential Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, (Executive Order 13800) and OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This Risk Report comprises the determination report and action plan required by Executive Order 13800, and is accordingly comprised of the following sections:

- **Executive Summary: Understanding Cyber Risks** – This section provides an overview of the findings and determinations discussed in this Risk Report and discusses four planned actions that OMB considers essential to effectively addressing systemic cybersecurity risk management challenges across the Government.
- **Risk Assessment Scope and Methodology** – This section describes OMB's methodology for assessing agencies' cybersecurity programs and preparing this Risk Report in coordination with the Department of Homeland Security (DHS).
- **Findings** – This section provides OMB's evaluation of 96 agency risk management assessment (risk assessment) reports, and describes planned actions that OMB and agencies will take to address government-wide cybersecurity gaps and identify unmet budgetary needs.

This Risk Report presents a high-level assessment of government cybersecurity risks, identifies actions to improve Federal cybersecurity, and acknowledges that OMB and the agencies must work together over the coming months to identify how to implement those actions. Together, these sections comprise the determination report and action plan required by Executive Order 13800.

Additionally, the Risk Report does not cover every risk identified in the agency risk assessments. Two of the most significant areas of risk that were identified in agency assessments were the abundance of legacy information technology (IT), which is difficult and expensive to protect, as well as shortages of experienced and capable cybersecurity personnel. Executive Order 13800 also requires the American Technology Council to produce an *Information Technology Modernization Report to the President* and for the Department of Commerce and DHS to produce a *National Cybersecurity Workforce Report to the President,* which will discuss these significant risks in greater breadth and scope. The Risk Report acknowledges these challenges and, in some instances, reinforces those reports. For instance, the Risk Report recognizes the detrimental impacts that limited personnel resources have on agencies' ability to manage their cybersecurity risks. It also examines the risks associated with several of the IT modernization challenges, namely decentralized security operations centers (SOCs) and the lack of standardized IT capabilities.

Executive Summary: Understanding Cyber Risks

Effective cybersecurity requires any organization — whether a private sector company, a non-profit, or an agency at the state, local, or Federal level — to identify, prioritize, and manage cyber risks across its enterprise. These cyber risks can manifest themselves in many ways, including the increasingly sophisticated techniques that threat actors use to compromise systems, the operation of outdated and unsupported IT, or the malicious links and email attachments that can infect unsuspecting users' machines with malware. The recent government-wide cybersecurity risk assessment process conducted by OMB, in coordination with the DHS, confirms the need to take bold approaches to improve Federal cybersecurity.

This Risk Report captures the results of the aforementioned government-wide risk assessment process, which examined agencies' ability to identify, detect, respond, and if necessary, recover from cyber intrusions, in accordance with Executive Order 13800. The actions discussed in this report aim to improve government-wide governance processes and implement cybersecurity capabilities "commensurate with risk and magnitude of the harm" that the compromise of a Federal information system and information would entail.

OMB and DHS determined that 71 of 96 agencies (74 percent) participating in the risk assessment process have cybersecurity programs that are either at risk or high risk. OMB and DHS also found that Federal agencies are not equipped to determine how threat actors seek to gain access to their information. The risk assessments show that the lack of threat information results in ineffective allocations of agencies' limited cyber resources. This situation creates enterprise-wide gaps in network visibility, IT tool and capability standardization, and common operating procedures, all of which negatively impact Federal cybersecurity.

OMB and DHS examined the performance of 96 agencies across 76 metrics, and this Risk Report identifies the following four (4) core actions that are necessary to address cybersecurity risks across the Federal enterprise:

1. Increase cybersecurity threat awareness among Federal agencies by implementing the Cyber Threat Framework to prioritize efforts and manage cybersecurity risks;
2. Standardize IT and cybersecurity capabilities to control costs and improve asset management;
3. Consolidate agency SOCs to improve incident detection and response capabilities; and
4. Drive accountability across agencies through improved governance processes, recurring risk assessments, and OMB's engagements with agency leadership.

This Risk Report describes OMB's plan to implement these actions with agencies over the coming year and reduce cybersecurity risks across the Government.

Risk Assessment Scope and Methodology

Executive Order 13800 requires all Federal agencies to submit risk assessment reports to OMB and DHS. Executive Order 13800 also requires OMB and DHS to assess those reports to determine whether the risk mitigation and acceptance choices set forth in the reports are appropriate and sufficient to manage the cybersecurity risk to the executive branch enterprise in aggregate. Executive Order 13800 also requires OMB, in coordination with DHS, to deliver a report to the President that includes the determination and a plan to adequately protect the executive branch, address unmet budgetary needs necessary to manage risk, establish a regular risk assessment process, and clarify and update policies, standards, and guidelines as necessary. Accordingly, this Risk Report provides findings on unmitigated risks that OMB identified after reviewing 96 agency risk assessments, while also describing a plan to address those risks.

Following the President's signature of EO 13800, OMB worked with partners from DHS, the National Institute of Standards and Technology (NIST), and other Federal agencies to develop valid and repeatable processes for risk determinations and conducting government-wide risk assessments. As a result of this work, OMB issued OMB Memorandum M-17-25, *Reporting Guidance for the Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* in May 2017 to detail the risk assessment process. The risk assessments leverage the Federal Information Security Modernization Act of 2014 (FISMA) Chief Information Officer (CIO) metrics from Fiscal Year (FY) 2017 and the Inspectors General (IG) metrics from FY 2016. Both sets of metrics align to the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST Framework), which provides a standard for managing and reducing cybersecurity risks.

The NIST Framework organizes cybersecurity capabilities around five functions: Identify, Protect, Detect, Respond, and Recover. Utilizing the NIST Framework in conjunction with NIST Special Publications 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View,* 800-37, *Risk Management Framework to Federal Information Systems,* and other NIST standards and guidelines, provides agencies with a comprehensive structure for making informed, risk-based decisions and managing cybersecurity risks across their respective enterprises.

OMB and DHS assessed agency performance across 76 metrics to determine the extent to which agencies are actively managing their cybersecurity risks. These 76 metrics include four narrative responses that indicate the extent to which an agency identifies and manages cybersecurity risks across the enterprise. OMB and DHS reviewed these metrics and made risk determinations of agencies' programs using the following schema:

- **High Risk:** Key, fundamental cybersecurity policies, processes, and tools are either not in place or not deployed sufficiently.
- **At Risk**: Some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain.

- **Managing Risk**: The agency institutes required cybersecurity policies, procedures, and tools and actively manages their cybersecurity risks.

The table below summarizes agencies' ratings in accordance with these assessment criteria:

Table 1: Agency Risk Management Performance

Managing Risk	At Risk	High Risk	Total
25	59	12	96

At the conclusion of the risk assessment process, OMB required each agency's Senior Accountable Official responsible for implementing Executive Order 13800 to submit a signed letter describing their agency's plan to accept, mitigate, avoid, or transfer cybersecurity risks in the near term. This Risk Report uses summary data from the agency metrics, narrative responses, and Senior Accountable Official letters to support findings and actions described herein. Additionally, OMB used information from its management and budget oversight processes to augment and contextualize the information in this Risk Report. OMB will continue to track the effectiveness of agencies' cybersecurity programs as part of an ongoing effort to implement Executive Order 13800.

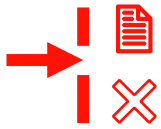
Findings and Planned Actions

Finding 1: Limited Situational Awareness

Finding: Agencies do not understand and do not have the resources to combat the current threat environment.

Action: OMB, DHS, and NSA will disseminate and help implement the Cyber Threat Framework to prioritize efforts and manage cybersecurity risks.

Government and industry cybersecurity reports and news headlines describing cybersecurity incidents continue to underscore that threat actors employ persistent and increasingly sophisticated techniques to attack and compromise information systems. Nevertheless, Federal agencies' and private organizations' ability to determine threat actors' motivations and methods for staging cyber-attacks has not improved. The risk assessment process revealed that those charged with defending agency networks often lack timely information regarding the tactics, techniques, and procedures that threat actors use to exploit government information systems. In fact, situational awareness is so limited that Federal agencies could not identify the method of attack, or attack vector, in 11,802 of the 30,899 cyber incidents (38 percent) that led to the compromise of information or system functionality in FY 2016.



38%

of Federal cyber incidents did not have an identified attack vector, suggesting limited situational awareness

Improving Situational Awareness

For the better part of the past decade, OMB, the Government Accountability Office (GAO), and agency IGs have found that agencies' enterprise risk management programs do not effectively identify, assess, and prioritize actions to mitigate cybersecurity risks in the context of other enterprise risks.[i] Furthermore, OMB found that only 59 percent of agencies reported having processes in place to communicate cyber risks across their enterprises. OMB has repeatedly emphasized that managing risk effectively requires timely data reporting and communication flows so that employees at all levels in the organization have the information necessary to block attacks in their area of responsibility.[ii]

59%

of agencies reported having processes in place to communicate cyber risks across their enterprises

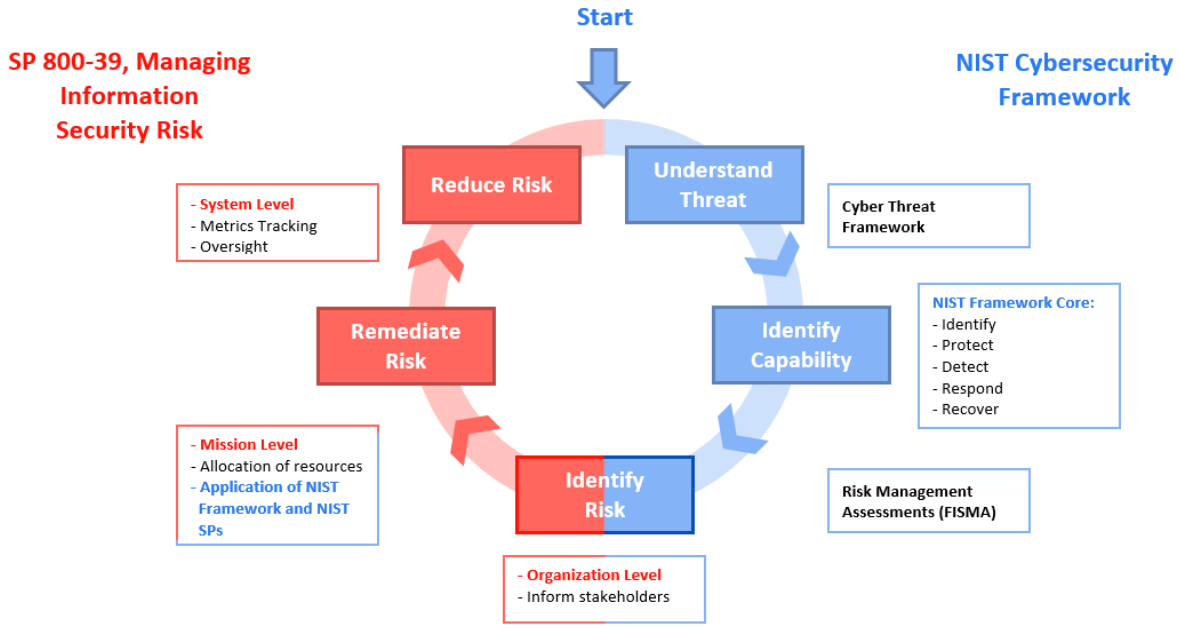
The agency risk assessments demonstrate that the Federal Government must implement a timely approach for communicating cyber threats and risks, and for

appropriately prioritizing the people, processes, and technology resources necessary to defend agency networks. To be effective, this approach must not only offer methods to provide situational awareness across agencies, but also focus on improving the existing frameworks used across government. Accordingly, over the next year OMB will work with DHS, the National Security Agency (NSA), and the Office of the Director of National Intelligence (ODNI) to disseminate and implement the Cyber Threat Framework, which provides decision makers at all levels with the insight and knowledge to make well-informed, prioritized cybersecurity investment decisions. This Cyber Threat Framework provides a hierarchical, structured, transparent, and repeatable methodology for characterizing adversarial activities in a standardized way across the Federal Government and helps foster a dialogue between leadership and cybersecurity professionals on methods to reduce cyber risk.

Cybersecurity professionals face challenges providing readily digestible information to senior leaders within their agency to manage their cybersecurity risk. Agencies can resolve this problem by using a common Cyber Threat Framework, which demonstrates the potential impact of current threats by using an analysis-driven, repeatable process to synchronize and balance cybersecurity investments, minimize redundancies, eliminate inefficiencies, and improve all-around mission performance. By using the Cyber Threat Framework, senior leaders will be able to recognize and effectively direct resources to mitigate cybersecurity risks. With this in mind, the NSA, Department of Defense CIO, and the Defense Information Systems Agency adopted the methodology of the Cyber Threat Framework as part of their Department of Defense Cybersecurity Assessment and Review (DODCAR).

The Cybersecurity Threat Framework also aligns with the NIST Framework functions and other NIST Special Publications. This alignment ensures the use of the common lexicon from the NIST Framework, while also providing tangible, risk-related outcomes for cybersecurity controls and capabilities. Figure 1 shows the relationship between the NIST Framework, NIST Special Publication 800-37, *Risk Management Framework to Federal Information Systems*, and the Cyber Threat Framework in the lifecycle of identifying, managing, and reducing cybersecurity risks.

Figure 1: Cyber Risk Management Lifecycle Management



Improving Resource Allocations

$5.7b

projected FY 2017 civilian agency cyber defense spending, versus $5.0b in FY 2016

In an effort to identify the unmet budgetary needs essential to managing cybersecurity risk to the Executive Branch enterprise, OMB assessed Federal agencies' responses and concluded that agencies must adopt a common approach to identifying risks, as well as budgeting for and allocating resources to address those risks. In the absence of a common approach, agencies continue to allocate their limited cyber funding to acquire single point solutions to provide capabilities for *perceived* security gaps, rather than allocating funds to address gaps that threat actors are *actually* exploiting. As a clear example, Federal civilian agencies project FY 2017 spending of $5.7 billion on cyber defenses across the NIST Framework functions, versus $5.0 billion in FY 2016, without a sense of prioritization or actual return on investment in terms of reducing cyber risks. While cyber spending increases year-over-year, OMB found that agencies are not effectively using available information, such as threat intelligence, incident data, and network traffic flow data to determine the extent that assets are at risk, or inform how they to prioritize resource allocations.

To address this issue, OMB spent the past two years developing and refining a risk-based budgeting model that ties agencies' cybersecurity spending to the FISMA metrics process in order to identify capability and process gaps that pose risks to the agency.

OMB plans to disseminate the risk-based budgeting process in early FY 2018 to enable agency CIOs, Chief Information Security Officers (CISOs), and Chief Financial Officers (CFOs) to communicate cyber risks effectively across their agencies and to budget strategically for cyber capabilities that address the agency's most critical cybersecurity needs. To achieve this end, OMB built the model using a common industry and government approach for examining cyber risk, where risk is based on the likelihood and impact of an event occurring.

In its current form, the risk-based budgeting model associates the lack of agency capabilities as perceived risk, although it does not assess the actual likelihood of those risks materializing. Incorporating the Cyber Threat Framework approach into this process will allow a given agency to identify strengths and weaknesses in its security defenses, and also identify redundant capabilities deployed across its network. This will ensure that agencies move away from implementing capabilities based on perceived agency risk and identify the extent to which they have strong or weak capability coverage to detect and defeat known threats. This will also provide a clear return on investment for cyber capabilities, as each dollar spent should block the most likely and most damaging threats and risks to the agency.

The Cyber Threat Framework shows the adversary life cycle including adversary objectives, adversary actions, and measurable indicators of the attack, as seen in Figure 2 and Figure 3.

Figure 2: ODNI Cyber Threat Framework High-Level View

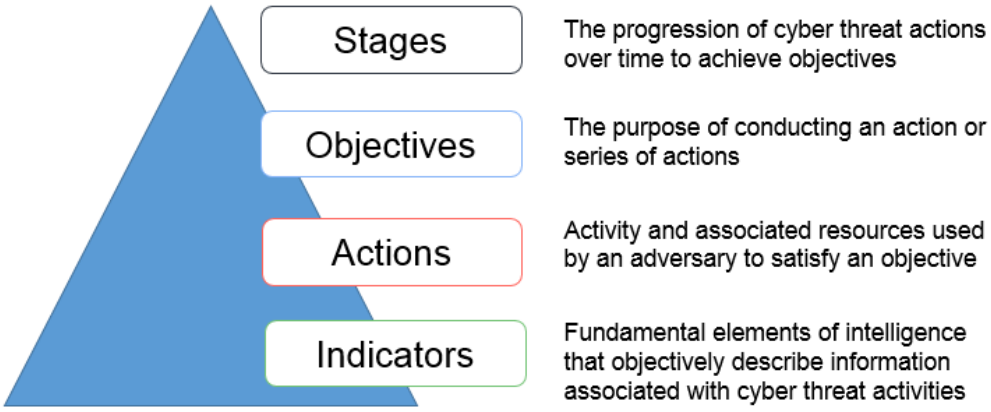
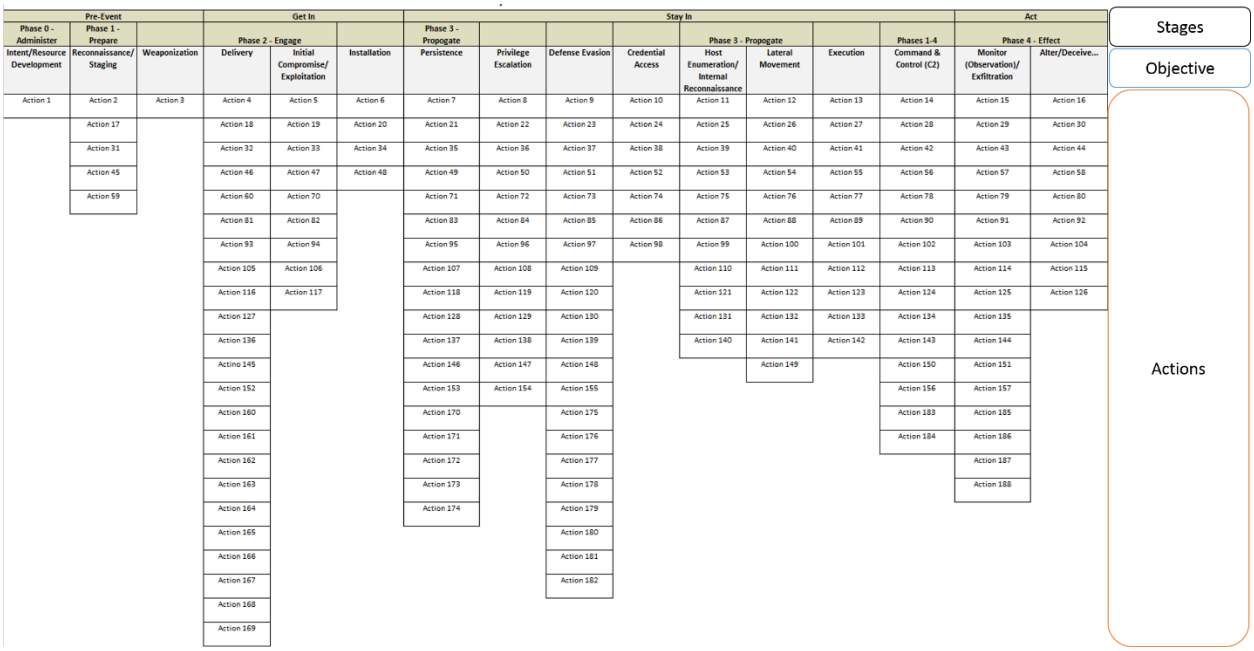
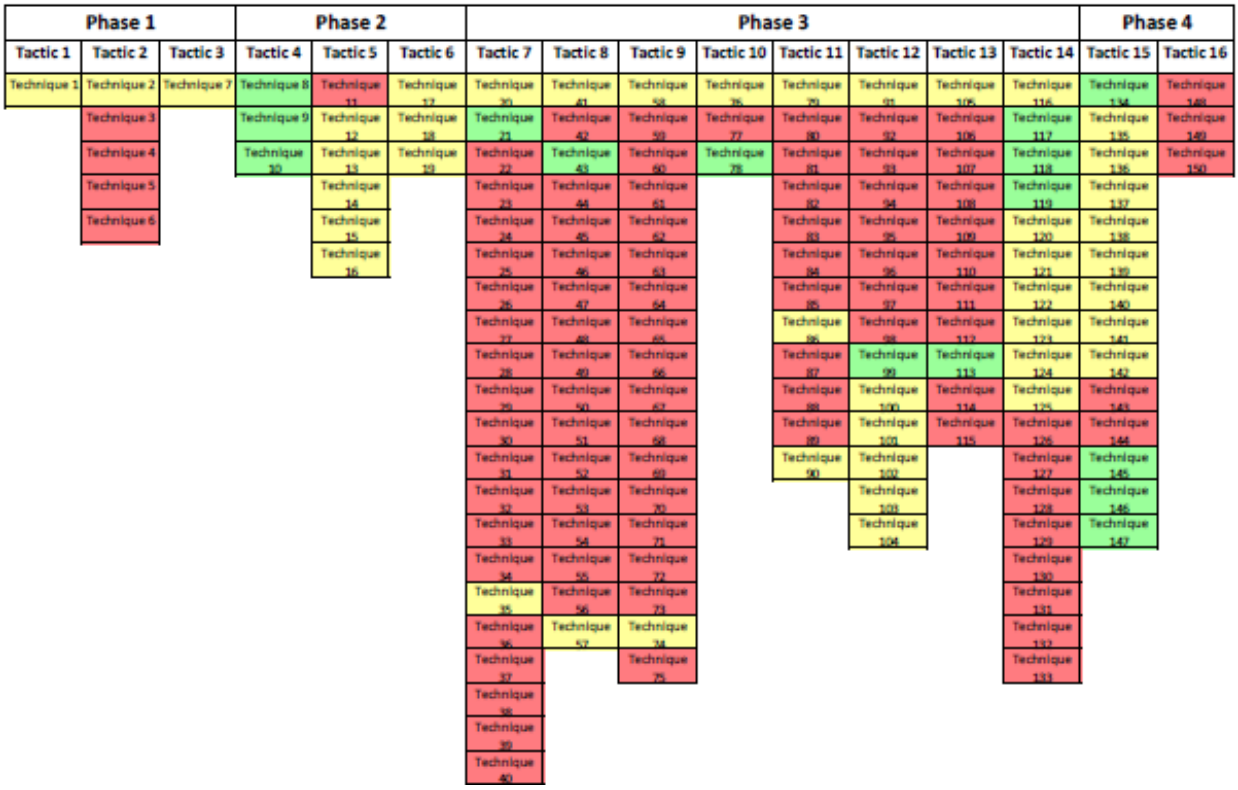


Figure 3: DODCAR Technical Architecture and the Cyber Threat Framework's High-Level View



By leveraging the NIST Framework functions, the Cyber Threat Framework approach allows agencies to create a mitigation coverage map to evaluate how effectively each cybersecurity capability protects, defends, and responds to adversary actions. The Mitigation Coverage map uses modeled data flows to allow consumers to easily understand mitigation coverage. The colors in the mitigation coverage map depict capability areas of strength, weaknesses, or gaps. The mitigation coverage map shows the highest level of coverage across all enabled capabilities within a data flow. A green color of Adversary Action means that there is at least one capability that mitigates that threat at a 'Significant' level, and there may or may not be several Moderate/Limited scores associated with that adversary action. A yellow color of Adversary Action means that there is at least one capability that mitigates that threat at a 'Moderate' level, and there may or may not be several Limited scores associated with that adversary action. A pink color of Adversary Action means that there is at least one capability that mitigates that threat at a 'Limited' level and red indicates there are no capabilities mitigating that threat action. Figure 4 provides a sample Cyber Threat Framework Mitigation Map.

Figure 4: DODCAR Cyber Threat Mitigation Map



This mitigation coverage map allows agencies to prioritize where they should allocate resources to address the most critical threats. OMB will work with DHS and NSA to socialize this framework and associated tools over the next year with the intent to have agencies prioritize their risk mitigation activities at the outset of FY 2019.

Finding 2: Lack of Standardized IT Capabilities

Finding: Agencies do not have standardized cybersecurity processes and IT capabilities, which impacts their ability to efficiently gain visibility and effectively combat threats.

Action: Agencies will continue standardizing their IT offerings and cybersecurity capabilities in FY 2019.

An agency's ability to mitigate security vulnerabilities is a direct function of its ability to identify those vulnerabilities across the enterprise. Agency risk assessments show that this issue becomes more complex in federated agencies, where there are not standardized procedures or technology across the organization is lacking. The lack of standardization and access to common capabilities means that these agencies cannot apply a single solution to address specific cybersecurity challenges and eventually reduce their overall attack surface. Although Congress and the Executive Branch have taken steps to enhance CIO authorities and visibility into IT spending across the organization through the Federal Information Technology Acquisition Reform Act (FITARA), the risk assessments demonstrate that additional actions are necessary to modernize and standardize IT solutions across the Government. Additionally, while agencies plan to utilize DHS's Continuous Diagnostics and Mitigation (CDM) program, which provides standardized capabilities aimed at enhancing visibility and eventually control costs, the risk assessments show that there are considerable capability gaps across government whose closure is necessary to ensure CDM's effectiveness over time.

Improving Access Management

One of the most significant security concerns that results from the current decentralized and fragmented IT landscape is ineffective identity, credential, and access management (ICAM) processes. Fundamentally, any organization must have a clear understanding of the people, assets, and data on its networks. Effective access management provides a governance structure that allows organizations to limit users' access to only the information required to perform their jobs, and therefore minimizes the risks of unauthorized access or information disclosures. To this end, Federal agencies have made tremendous progress enforcing the use of multi-factor authentication Personal Identity Verification cards in recent years. Through increased oversight, and accountability for implementing this control, agencies now enforce the use of this control among 93 percent of their privileged users, users who have access to large tranches of sensitive agency and citizen data. While agencies have been successful in implementing multi-factor authentication

93%

of users have enforced usage of Personal Identity Verification cards

controls, agencies have not matured their access management capabilities or optimized their architectures to enable effective ICAM programs across the enterprise.

To continue progress, the Federal agencies must improve their ICAM architecture through the centralization of such solutions. In particular, agencies need to move toward a single, authoritative solution for establishing and managing attribute- or role-based access controls for their users. OMB found that, across government, agencies employ fragmented ICAM programs, solutions, and user directories. This structure prevents agencies from achieving a comprehensive understanding of their users, managing those users' access to the agency network, and effectively safeguarding sensitive government information. For example, one agency noted that it maintains a decentralized environment with 23 domains and over 300 unique user groupings based on geographic location, which precludes the agency from effectively managing users' access to information across the enterprise.

Furthermore, the IGs report that only 55 percent of agencies limit access based on user attributes and roles and only 57 percent review and track administrative privileges. Although effective ICAM is a foundational step to ensuring that the right users have access to the right data at the right time, only half of Federal agencies have processes in place to restrict users' access to information. Over the next year, OMB and DHS will work to enhance agencies' access management programs, starting with efforts to provide enterprise-wide views of who is on their networks.

Email Consolidation

Email, by way of phishing attacks, remains one of the most common attack vectors across both government and industry. The 23 civilian CFO Act[iii] agencies combine to have nearly 2.2 million email inboxes, with hundreds of thousands of additional inboxes across 100+ small agencies. Standardizing and consolidating email at the enterprise level is a key element of the strategy for securing users, and yet some agencies report several separately managed email services inside their organizations. For example, one agency lists no fewer than 62 separately managed email services in its environment, making it virtually impossible to track and inspect inbound and outbound communications across the agency.

Standardizing email services across the agency enhances the ability to provide phishing protection by inspecting inbound and outbound messages, disabling and quarantining malicious attachments, and validating the sender and receiver in email exchanges. At least nine of the 23 CFO Act agencies have already consolidated their enterprise email and note that associated complexities stem from the size of the organization, rather than from cost or technical challenges. In fact, the largest of these agencies, with over 100,000 users, estimates a 10-month timeframe for consolidating all of their users into a single email solution. Additionally, agencies of varying size that have consolidated, or that are in the process of consolidating, their email services identify cost savings in the $1 million to $4 million range per year. Accordingly, over the coming year, OMB will work with agencies to develop enterprise-wide email consolidation plans in support of the activities set forth in the *IT Modernization Report to the President*.

Standardized Software and Applications

49% >_

of agencies have the ability to detect and whitelist software running on their systems

Several industry reports identify software application whitelisting as one of the most critical cybersecurity controls for preventing, or minimizing the impact of, cyberattacks. Software whitelisting is a process by which agencies list applications and application components that are authorized for use in an organization. This capability is especially effective for those attacks that employ malware and malicious code. IGs consistently find that agencies are limited in their ability to detect and whitelist the software running on their systems, with only 49 percent of agencies having this capability. In addition to not actively whitelisting software, many agencies have multiple versions of the same software tools in place, or they have tools that have overlapping functionality. Different versions of the same software will often have distinct vulnerabilities and require unique efforts from an agency's security team(s), whose time is better spent on standard implementations. In the absence of this capability, agencies do not have a clear picture of the applications running on their networks.

To address the difficulty and complexity of securing multiple versions of the same software tool, or competing tools in the same environment, OMB and the General Services Administration (GSA) will work with agencies to move to standard configurations or versions through shared services and new government-wide marketplaces. This effort will augment the software application whitelisting capability that DHS is providing to agencies in CDM Phase 1. These initiatives are critical to allocating resources effectively during the acquisition process and, more broadly, in securing the Federal environment as a whole.

Finding 3: Limited Network Visibility

Finding: Agencies lack visibility into what is occurring on their networks, and especially lack the ability to detect data exfiltration.

Action: Agencies will begin consolidating their Security Operations Center capabilities and processes, or migrating to a SOC as a Service in FY 2019.

Federal agencies do not have the visibility into their networks to effectively detect data exfiltration attempts and respond to cybersecurity incidents. The risk assessment process revealed that 73 percent of agency programs are either at risk or high risk in this critical area. Specific metrics related to data loss prevention and exfiltration demonstrate even greater problems, with only 40 percent of agencies reporting the ability to detect the encrypted exfiltration of information at government-wide target levels. Only 27 percent of agencies report that they have the ability to detect and investigate attempts to access large volumes of data, and even fewer agencies report testing these capabilities annually. Simply put, agencies cannot detect when large amounts of information leave their networks, which is particularly alarming in the wake of some of the high-profile incidents across government and industry in recent years.

27%

of agencies reported that they have the ability to detect and investigate attempts to access large volumes of data

The risk assessments also reveal that agencies have a low level of maturity on incident response as a whole. Only 52 percent of agencies reported having validated incident response roles during testing over the past year. Agency IGs also found that only 30 percent of agencies have predictable, enterprise-wide incident response processes in place, with as few as 17 percent of agencies actually analyzing incident response data after an incident has occurred. This indicates that agencies are not adequately developing incident response processes and, when incidents occur, they are not able to respond in a consistent manner.

The current situation is untenable, as agencies lack both the visibility into their networks to determine the occurrence of cybersecurity incidents and the ability to minimize the impact of an incident if one is detected. In the near term, the DHS CDM program seeks to provide agencies with greater insights into what is occurring on their networks. Specifically, the program will include access management capabilities, as well as boundary protection and event management capabilities in Phases 2 and 3, respectively. Although DHS expects to onboard these tools in FY 2018, the CDM program is hampered by delays due to a series of government-wide and agency-specific implementation challenges. Phase 1, which DHS initiated in 2015, focuses on hardware, software, vulnerability, and secure configuration management and DHS will continue working with all participating agencies to complete implementation. At this stage in Phase 1 deployment, 62 percent of agencies have capabilities in place through

CDM to understand the devices accessing their networks to ensure they are authorized to be connected, properly configured, and free of unpatched vulnerabilities. Phase 2, originally planned for full deployment by December 2016, is now being deployed.

CDM is one part of a larger effort to standardize, centralize, and provide visibility of agency cybersecurity capabilities across the enterprise. Agency SOCs use the CDM capabilities and incident response processes to provide centralized visibility into the state of security across an agency's network(s) by continuously monitoring for malicious or anomalous behavior and acting as first responders in the case of an event or incident. However, many Federal agencies report that they do not have sufficient full-time employees with the requisite skills to operate a SOC effectively, or, in some cases, agencies have multiple SOCs that employ a series of different processes and technology. The result is poor network visibility and inefficient and ineffective operations.

In the case of agencies with multiple SOCs, CISOs report that these SOCs do not communicate with each other and that they hoard, rather than share, threat information and intelligence. Although OMB previously worked to alleviate this issue by having agencies designate a principal SOC,[iv] which would be accountable for all incident response activities for each agency, it is clear that the problem persists. Accordingly, OMB and DHS will work with agencies over the remainder of FY 2018 to establish plans for consolidating SOC operations across their enterprise. SOC consolidation does not necessarily mean moving all resources to a single location, as such a move can create a single point of failure in an agency's security. Instead, SOC consolidation focuses on centralizing information sharing across the enterprise, while conducting the appropriate work (e.g., vulnerability and patch management) at a regional or local level.

While a lack of centralized SOC operations is a concern at several of the federated agencies, an even greater concern is those agencies with underperforming SOCs or those that do not have SOC capabilities at all. More than 70 percent of agencies report spending under $1 million on cybersecurity capabilities in this area, which indicates a significant number of agencies are unable to dedicate the personnel and resources to defending themselves from malicious cyber activity. To remedy this situation, and in line with the deadlines set forth in the *IT Modernization Report to the President*, OMB, in coordination with DHS, will explore designating at least one agency a SOC Center of Excellence, and select agencies to provide SOC as a Service offerings for use across the Federal Government. Each selected agency will provide a plan to appropriately scale their SOC operations to provide these capabilities to other agencies along with a pricing model. At the same time, OMB, in coordination with DHS and GSA, will work with agencies to determine which agencies will migrate to a SOC as a Service provider. OMB will coordinate with DHS and work with additional agencies to migrate underperforming agencies to a SOC as a Service model following analysis of SOC capability information.

Finding 4: Lack of Accountability for Managing Risks

Finding: Agencies lack standardized and enterprise-wide processes for managing cybersecurity risks.

Action: Hold agency heads accountable for their organization's security and governance processes, by conducting quarterly risk assessments that track agencies' progress implementing cybersecurity controls.

Both FISMA and Executive Order 13800 identify the agency head as the official ultimately responsible for each agency's cybersecurity. FISMA also requires agencies to report their cybersecurity program performance to the OMB Director. OMB uses this information as part of its oversight processes to ensure that agency heads efficiently and effectively safeguard their networks and protect taxpayers' information from cybersecurity risks. While such top-level accountability is important to drive measurable improvements agency-wide, agency heads often delegate cyber risk management responsibilities to the CIO and CISO. While most agencies noted in their responses to Executive Order 13800 that their leadership was actively engaged in cybersecurity risk management, many did not, or could not, elaborate in detail on leadership engagement above the CIO level.

This finding is concerning because the assessments show that CIOs and CISOs often lack the authority necessary to make organization-wide decisions despite direction to centralize authority in statutes such as FITARA and FISMA. This is particularly true in federated agencies, which employ multiple component CIOs who often control their own budgets. OMB and the IGs have repeatedly found that senior-level visibility and authority is necessary to drive consistent improvement in agency cybersecurity, and requires the agency head, Deputy Secretary, and CXOs to be involved and prepared to hold underperforming components accountable. However, the agency risk assessments, OMB's oversight processes, and IG and GAO reports all show that awareness and accountability for managing cyber risks is uneven across the Federal enterprise.

Additionally, IGs report that Federal agencies possess neither robust risk management programs nor consistent methods for notifying leadership of cybersecurity risks across the agency. In contrast to Federal agencies' approach to transparency and accountability, the Securities and Exchange Commission requires every publicly-traded company to file quarterly 10-Q and annual 10-K reports to inform shareholders of risks, including cyber risks that could affect their business. These reports are meant to demonstrate the due diligence and due care companies undertake to safeguard their business operations and shareholder's investments. Federal agencies would benefit from a similar process that tracks quarterly performance against strategic performance targets, communicates the resulting risks to stakeholders, and provides a sense of the return on investment for cybersecurity protections over time.

Accordingly, OMB will work across Government to enhance agency leadership's oversight of, and engagement in, their agency's cybersecurity program. To ensure agency leadership is regularly apprised of the state of cybersecurity in their organization, OMB will require CFO Act agencies to submit risk assessments on a quarterly basis, and OMB will provide results of these assessments to agency Deputy Secretaries through the President's Management Council. Small agencies will also participate in this process on a semi-annual basis.

OMB will also use its enhanced visibility into agency cybersecurity spending to ensure agencies are investing in priority cybersecurity protections. This improved understanding of agency activities comes from OMB's effort to align performance capabilities with budgeting activities, allowing for a common vocabulary and understanding as agencies discuss their investments in security capabilities. For instance, there have been repeated calls from industry leaders, GAO, and privacy advocates to make more robust use of data-level protections, including the encryption of data both at rest and in transit. However, while agency encryption of data in transit is fairly secure, with 73 percent of agencies reporting full implementation, less than 16 percent of agencies achieved the target for encrypting data at rest.[v] Agencies have demonstrated that this is a low priority. Non-defense Federal agencies budgeted less than $51 million on encrypting data at rest in FY 2017, among the lowest of any cybersecurity capability, with 50 percent of this budget coming from two agencies. Compare this to the almost $210 million agencies have budgeted for attaining and renewing authorities to operate for their systems, and it is easy to see government's priorities must be realigned.

16%

of agencies achieved the Government-wide target for encrypting data at rest

Conclusions

At a time when our reliance on technology is becoming greater and the Nation's digital adversaries are growing more adept, we must ensure that the Federal Government can secure citizens' information and deliver on their core missions. To this end, the Risk Report has identified four core actions to enhance government-wide cybersecurity risk management practices in a timely manner. In the near term, OMB will take necessary actions to implement the Cybersecurity Threat Framework, standardize IT capabilities and tools, consolidate or migrate SOC operations, and drive accountability for cybersecurity risk management across the enterprise. These actions will help shape agency budgets for FY 2019 and beyond. OMB will continue to work with its cross-agency partners, including DHS, NIST, GSA, and others to ensure that agencies are aware of expectations and available resources. Additionally, OMB will work through the Federal CIO and CISO Councils to ensure that the Federal Government is moving together toward improved security outcomes.

Appendix A: Acronyms

Acronym	Explanation
CDM	Continuous Diagnostics and Mitigation Program
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CXO	Collective of Executive Officers
DHS	Department of Homeland Security
Executive Order 13800	Presidential Executive Order 13800, Strengthening the Cybersecurity of Federal Network and Critical Infrastructure
FISMA	Federal Information Security Modernization Act of 2014
FITARA	Federal Information Technology Acquisition Reform Act
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
ICAM	Identity, Credential, and Access Management
IG	Inspectors General
IT	Information Technology
NIST	National Institute of Standards and Technology
NIST Framework	National Institute of Standards and Technology's *Framework for Improving Critical Infrastructure Cybersecurity*
NSA	National Security Agency
DODCAR	Department of Defense Cybersecurity Analysis and Review
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
SOC	Secure Operations Center

Endnotes

[i] For more information see GAO *Cybersecurity: Actions Needed to Strengthen U.S. Capabilities*, February 14, 2017 and OMB *FY 2016 FISMA Report to Congress*, March 10, 2017.

[ii] OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, for additional guidance on managing enterprise risks, see the *Enterprise Risk Management Playbook* for additional information.

[iii] Chief Financial Officer (CFO) Act Agencies – CFO Act agencies are those agencies designated in the CFO Act (with the addition of DHS and minus the Federal Emergency Management Agency). In practice, the CFO Act agencies are the 24 largest Federal agencies in terms of budget; the 23 civilian CFO Act agencies are the CFO Act agencies less the Department of Defense.

[iv] OMB Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*.

[v] Per *NIST SP 800-53r4, Security and Privacy Controls for Federal Information Systems and Organizations*, information at rest refers to the state of information when it is located on storage devices as specific components of information system (SC-28); data in transit refers to refers to information as it moves between endpoints.