THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Secure Government Communications

August 20, 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Revolutionary technological changes—including shared and dispersed cloud computing capabilities; mobile computing devices and smart phones; increased use of social media; and interdependencies of computing systems—are exploding across the electronic communications landscape and are being adopted at a rapid pace in both public and private sectors.

In this new environment, continuous access to data has become central to mission performance across all operational lines; however, just as technological advancement can yield benefits (e.g., enhanced access, efficiencies, and cost savings), mission reliance on data also elevates risks and consequences of data security. These advancements have introduced thousands of applications, threats, and vulnerabilities into communications networks, which are increasingly hidden from traditional network security devices. Given organizations' reliance on these advancements to conduct even basic business functions, cyber threats that previously only affected a small fraction of business activities are beginning to impact all sectors and business functions.

Data ubiquity has also shifted the behavior of the technology's end users and network security professionals. For example, many modern applications and services enable users to access their data from any location and any device in near real time. To achieve this ubiquity, data is often stored at locations known only to the service provider, making it unprotected by legacy enterprise security strategies. Each of these behaviors requires a new approach to operational security strategies and risk management. Solely securing network perimeters is no longer an effective method to address dispersed computing platforms, greater worker mobility, and social media.

Recognizing the tension between advances in technology capabilities and more aggressive threat behavior, leading industry organizations have developed novel approaches to security to successfully operate in this environment. These approaches demand new thinking and refined technologies, behaviors, and organizational constructs.

In 2012, the National Security Staff requested that the President's National Security Telecommunications Advisory Committee (NSTAC) investigate how a higher degree of integrity, confidentiality, and availability could be attained by implementing industry best practices, commercial off-the-shelf tools, and/or managed security services. To set parameters around its research, the NSTAC only examined developments that occurred since 2007. Several related conditions for unclassified Government systems that have become prominent since 2007 include:

- Revolutionary technologies (e.g., smartphones, cloud, tablets) that signified the advent of remote access and data mobility;
- Cloud computing for the exchange and storage of sensitive-but-unclassified and unclassified information;
- The interdependencies of networked systems, resulting in higher potential consequences from successful events; and

- The significant rise in malicious activity against U.S. targets by well-funded and supported entities leading to the emergence of advanced persistent threats (APT).

To inform its research, the NSTAC engaged subject matter experts and thought leaders across a wide range of industries and companies, including some of the world's top information technology (IT) organizations, information security firms, and consumer-focused enterprises.[1] The committee also heard from Federal Government data security experts and program leaders and reviewed past Government and private sector advisory panel recommendations, and other reports and testimonies.

While analyzing both the Government's current approach to its cybersecurity environments, challenges, and requirements, and industry's innovative, novel security approaches, the NSTAC's insights coalesced around three essential elements that are needed to enhance communications security: technology, behavior, and organization. Each element has an essential role in in addressing a specific subset of security challenges facing industry and Government today:

- Technologically, a more dispersed enterprise means that data is more often in transit to/from, and resident on, a greater variety of devices; further, the more abstract data perimeter broadens the surface that the Government must protect.
- Behaviorally, a more mobile workforce means the usage of additional computing platforms, many of them personally-procured and managed; the lack of appropriate user training can have cascading impacts.
- Organizationally, dispersed authority for cybersecurity can yield inconsistent compliance, uneven implementation of responses, and diluted accountability for real-time, long-term security standards and processes.

As a result of its examination, the NSTAC strongly advocates for a balanced and holistic program of technological modernization, behavioral reinforcement and guidance, and organizational adaptation to maximize results and manage processes. The NSTAC found that novelty is achieved by simultaneously implementing the solutions across the three related domains. Specific solutions include:

- Technological Solutions: The NSTAC identified several technological advancements that would be beneficial and effective to help secure Government information, including the use of large-scale data analytics, white/black listing, and containerization, among others. When combined, these practices form the basis of cybersecurity and risk regimes implemented by many corporations under current conditions.

- Behavioral Solutions: Recognizing technology as the driver behind behavioral patterns, the NSTAC determined that creating a culture of security through training is imperative for effective risk and consequence management. In addition to offering employees appropriate incentives, cyber training provides communities working in and with the Government the situational awareness needed to help reduce threat consequence and provides one of the

[1] For a complete listing of subcommittee briefings, see Appendix D.

highest returns on investment for defending Government communications. Leadership commitment and vision is also critical to drive success.

- Organizational Solutions: The NSTAC found that the relationship between IT and an organization's management is improved when leading industrial organizations and Government thinkers recognize that the nature of IT is central to organizational performance. Additionally, leading companies are evolving their organizational structures, as well as the responsibilities and status of those who manage risk, both in IT and throughout the organization. With technological interdependencies now enabling secure mission performance across an enterprise, modern industry leaders manage risk-associated processes that extend far beyond the historic scope of IT and telecommunications.

Based on the authorities and responsibilities established by Executive Order13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, the NSTAC presents the following multi-pronged recommendation to the President:

- Direct an appropriate organization to develop, adopt, and implement an integrated and balanced plan across the technological, behavioral, and organizational domains reflecting a unified strategy for more secure Government communications, as described below. Advancing in each of these three areas is not simply synergistic, but rather symbiotic; the central understanding is that the power of the strategy is only achieved by simultaneous, balanced, and coherent implementation of change in all three domains.

  The elements of this unified strategy and their related recommendations include:

  1. <u>Technology: Creating New Cybersecurity Strategies</u>

     Modernize network security technology and adopt data-centric technology approaches to prioritize and protect data.

     – Implement security technologies and techniques providing for network defense-in-depth, embracing net users, devices, data, and applications wherever located with strong and comprehensive policy oversight and adaptive controls.

     – Upgrade legacy network security technology with currently available next generation security technologies and associated processes, as defined herein, throughout Federally-managed networks; implementation to be prioritized based on elevated risk and consequence management processes discussed in this report.

     – Employ automated data analytics designed to achieve real-time contextual cybersecurity.

  2. <u>Behavior: Expanding a Culture of Security</u>

     Instill in every member of every Federal organization his or her identity as a full, active, and accountable participant in organizational cybersecurity.

     – Expand policies and standards to embrace all technologies and users accessing Federal networks.

- Monitor, test, and evaluate all organizations and users for adherence to cybersecurity policy and standards on a rigorous and continuous basis.
- Institutionalize the review and revision of behavioral policies and technology standards with frequency predicated on changing technology and the threat environment.

3. Organization: Elevating Risk and Consequence Management

Elevate and qualitatively change IT and its security to become central to mission performance within each organization.

- Expand the scope of security processes beyond traditional IT to the full scope of risk management as defined herein.
- Across that full scope, establish a single centralized organization with responsibility, authority, and accountability across the Executive Branch.
- Replicate this process in every Federal organization at the agency-level.
- Employ this cross-governmental organization to create a comprehensive, unified risk management strategy across the Federal Government within 12 months.

1.0 INTRODUCTION

What Has Changed?
Revolutionary technology is exploding across the communications field and is rapidly being adopted in both public and private sectors, changing the landscape of risk and vulnerability.

Revolutionary technological changes are exploding across the communications landscape, being adopted at a rapid pace in both public and private sectors. A Virtustream report found that the majority of U.S. businesses are now using some form of cloud computing to support information technology (IT), and IT research firm Gartner predicts that 70 percent of mobile professionals in industry will perform work on personal smart devices by 2018.[2,3] As depicted in Figure 1, the pace of adopting new computing platforms reflects the exponential growth in the creation of digital content, including information that is publicly shared, tagged, and searchable.

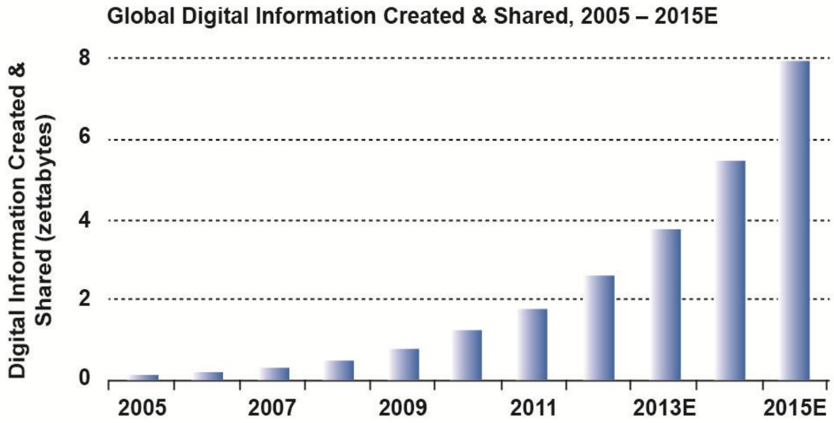


Figure 1: The Growth in Digital Information Created and Shared[4]

In this new environment, continuous access to data has become central to mission performance across all operational lines; however, just as technological advancement can yield benefits (e.g., enhanced access, efficiencies, and cost savings), mission reliance on data also elevates the risks and consequences of data security. These advancements have introduced thousands of applications, threats, and vulnerabilities into communications networks, which are increasingly hidden from traditional network security devices. Given organizations' reliance on these advancements to conduct even basic business functions, cyber threats that previously only affected a small fraction of business activities are beginning to impact all sectors and business functions.

Data ubiquity has also shifted the behavior of the technology's end users and network security professionals. For example, many modern applications and services enable users to access their data from any location and any device in near real time. To achieve this ubiquity, data is often stored at locations known only to the service provider, making it unprotected by legacy

[2] Cohen, Reuven. "The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing." *Forbes*. April 16, 2013. Available: http://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing/.
[3] Willis, David A. "Bring Your Own Device: The Facts and the Future." *Gartner*. April 11, 2013.
[4] Gants, John and David Reinsel. "Extracting Value from Chaos." *IDC*. June 2011.

enterprise security strategies. Each of these behaviors requires a new approach to operational security strategies and risk management. In today's threat environment, solely securing network perimeters is no longer an effective method to address today's dispersed computing platforms (cloud computing), greater worker mobility and remote access, and social media (see Figure 2).

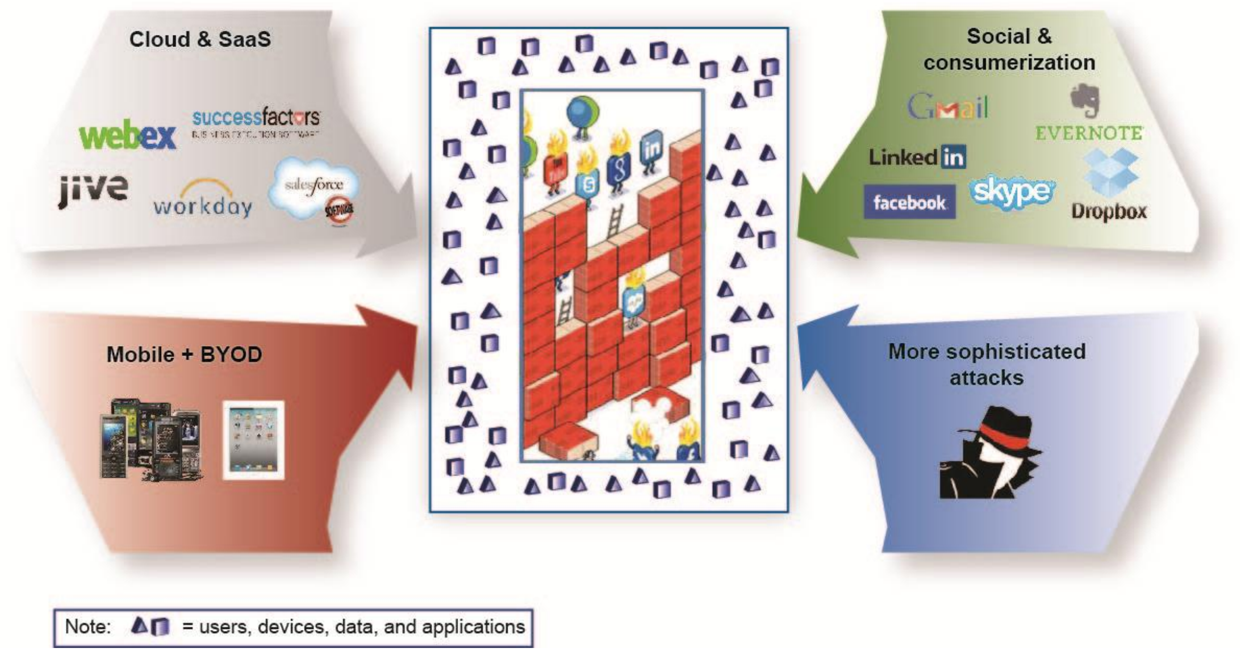


Figure 2: The New World of Data Ubiquity

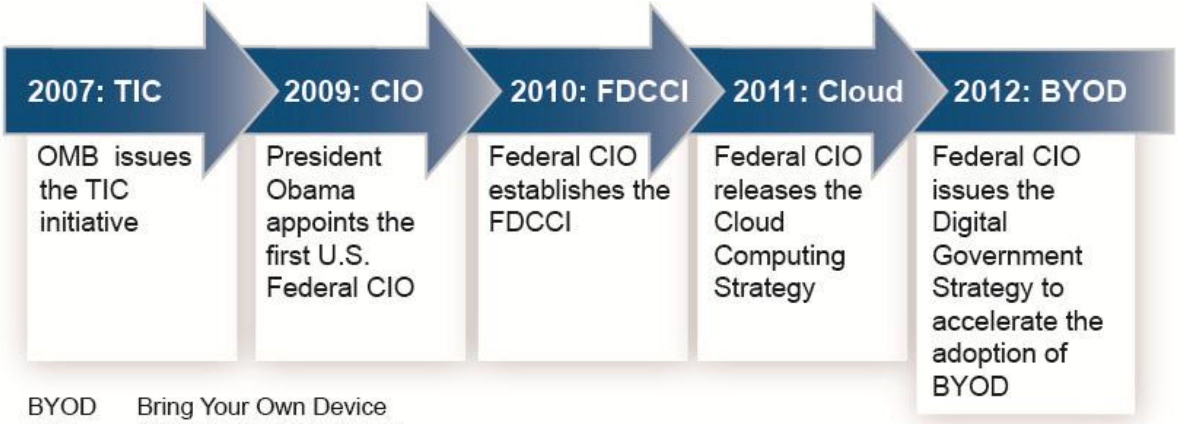
The Federal Government has not been exempt from the increased security implications of evolving technologies.[5] To mitigate these new threats, the Federal Government enterprise (i.e., the .gov domain) must adapt in ways that provide innovative, coordinated, and sustained responses across the Government.[6] The Government has attempted to address data ubiquity and the associated challenges through policy, including the Cloud First Policy, the *Federal Cloud Computing Strategy*, and the Federal Risk and Authorization Management Program (FedRAMP)[7] (see Figure 3). Despite the Federal policies in place and the severity of the threats, there are still disparities in how Federal departments and agencies (D/A) approach network security. For example, each major Federal D/A has its own chief information officer (CIO) and chief information security officer (CISO) that operate independently of their counterparts in other Federal D/As. Additionally, although there are mechanisms for collaboration and

[5] According to the Government Accountability Office (GAO), Federal D/As have experienced a significant rise in security incidents. From 2006 to 2012, the GAO reported that cybersecurity incidents against the Government increased by 782 percent. Source: GAO. *Cybersecurity: National Strategy, Roles and Responsibilities Need to Be Better Defined and More Effectively Implemented*. February 2013. Available: http://www.gao.gov/assets/660/652170.pdf.

[6] Jackson, William. "Will Agencies Get Squeezed on Cybersecurity Technology?" *Government Computer News.* March 8, 2013. Available: http://gcn.com/blogs/cybereye/2013/03/agencies-squeezed-cybersecurity-technology.aspx.

[7] Office of Management and Budget. U.S. Chief Information Officer. *Federal Cloud Computing Strategy*, February 8, 2011. Available: https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

consultation, each D/A has its own tools, processes, security operations center or outsourced service provider, and independent budgets.


2007: TIC
OMB issues the TIC initiative
2009: CIO
President Obama appoints the first U.S. Federal CIO
2010: FDCCI
Federal CIO establishes the FDCCI
2011: Cloud
Federal CIO releases the Cloud Computing Strategy
2012: BYOD
Federal CIO issues the Digital Government Strategy to accelerate the adoption of BYOD

BYOD	Bring Your Own Device
CIO	Chief Information Officer
FDCCI	Federal Data Center Consolidation Initiative
OMB	Office of Management and Budget
TIC	Trusted Internet Connections

Figure 3: Evolution of Government Initiatives to Adapt to Technological Change Since 2007

While further progress is still needed to protect all Federal networks, leading industry and Government officials have mitigated and managed aspects of this new threat and risk environments through novel security approaches. Throughout its investigation, the President's National Security Telecommunications Advisory Committee (NSTAC) has examined many of these novel approaches, as well as the Government's current approach to its cybersecurity environments, challenges, and requirements. After extensive analysis, the NSTAC presents several recommended courses for Government action, described throughout this report, to help increase the security of Federal Government communications.

1.1 Background and Charge

In May 2012, the National Security Staff (NSS) requested that the NSTAC investigate how a higher degree of integrity, confidentiality, and availability of Governmental unclassified communications could be gained by adopting the best practices, approaches, and perspectives from the private sector and commercial marketplace. The NSS asked the NSTAC to consider the cost, security value, technical difficulty, and time to implement any proposed solutions.

Following this request, the NSTAC established the Secure Government Communications (SGC) Scoping Subcommittee in October 2012 to further define the goals of such an effort, and the NSTAC established the SGC Subcommittee in January 2013 to further examine this issue.

To set parameters around its research, the NSTAC only examined developments that occurred since 2007. Several related conditions for unclassified Government systems that have become prominent since 2007 include:

- Revolutionary technologies (e.g., smartphones, tablets) that signified the advent of remote access and data mobility;

- Cloud computing for the exchange and storage of sensitive-but-unclassified and unclassified information;
- The interdependencies of networked systems, resulting in higher potential consequences from successful events; and
- The significant rise in malicious activity against U.S. targets by well-funded and supported entities. (This activity is generally referred to as an advanced persistent threat [APT].)[8]

To effectively respond to this new environment, it was important to examine the threats, vulnerabilities, consequences, and costs that accompany these conditions, as well as the benefits of risk and consequence management.[9]

1.2 Study Method

To inform its research, the NSTAC engaged subject matter experts and thought leaders across a wide range of industries and companies, including some of the world's top IT organizations, information security firms, and consumer-focused enterprises.[10] The NSTAC received briefings on novel approaches in several significant areas, including new security strategies; the shift from perimeter security to data security; redesigned employee information security programs with incentives that create a culture of security; and an enterprise-wide approach to risk management incorporated under a unified strategy. The NSTAC also heard from Federal Government data security experts, program leaders, and organizations that have created risk management roles and risk committees. Finally, the NSTAC reviewed past Government and private sector advisory panel recommendations, other reports and testimonies, and ongoing governmental information security programs.

2.0 APPROACHING THE PROBLEM

Throughout its study, the NSTAC defined communications as the totality of users, devices, data, and applications on the modern network, and examined the interactions between these components and the resulting consequences. Noting the interaction between technology drivers, user behaviors, and consequences, the solution to enhancing communications security should be systemic across multiple operational elements and across all D/As.

At the highest level, the NSTAC addressed the following functions to better understand the current threat environment and industry's proposed novel approaches:[11]

[8] APT is any attack that passes an organization's existing defenses, can remain undetected once in place, and continues to cause damage. See: Pescatore, John. "Defining the Advanced Persistent Threat." *Gartner*. November 11, 2010. Available: http://blogs.gartner.com/john_pescatore/2010/11/11/defining-the-advanced-persistent-threat/.

[9] Consequence management is accomplished via methods used for increased resiliency such as system or asset redundancy, lowered dependence on other systems, fast recovery times, and infrastructure hardening. This approach might also require a de-coupling of infrastructures and services so that if a certain facility or function is disabled (via cyber or other means) its loss will have minimal impact on other facilities or functions that normally depend on it.

[10] For a complete list of subcommittee briefings and consulted works, see Appendix D.

[11] For a detailed discussion of these questions and summary of the NSTAC's response, see Appendix G.

- Prevention: How can the introduction of malware be most reliably prevented?
- Detection: How can threats be most reliably detected and understood?
- Containment: How can continuous analysis of the threat/response environment be used to tune security management to prevent malware, external attacks, or an insider threat from roaming through interconnected networks?
- Remediation: How can threats that circumvent all protections be most effectively removed, and any damage repaired?

The NSTAC's approach and response to these questions illuminated the Government's current cybersecurity environments, challenges, and requirements, as well as determined novel security approaches being implemented by certain organizations. These insights resulted in the recognition that no one security solution exists to address threats in the current cybersecurity environment; instead, the NSTAC identified three essential elements needed to enhance communications security, which can be characterized as **technological**, **behavioral,** and **organizational solutions**. When simultaneously implemented, these individual solutions create the basis of a unified strategy necessary to secure Government communications (see Figure 4). These elements are discussed in detail in Sections 3.0 and 4.0, and are also addressed in Sections 6.0, 7.0, and 8.0.

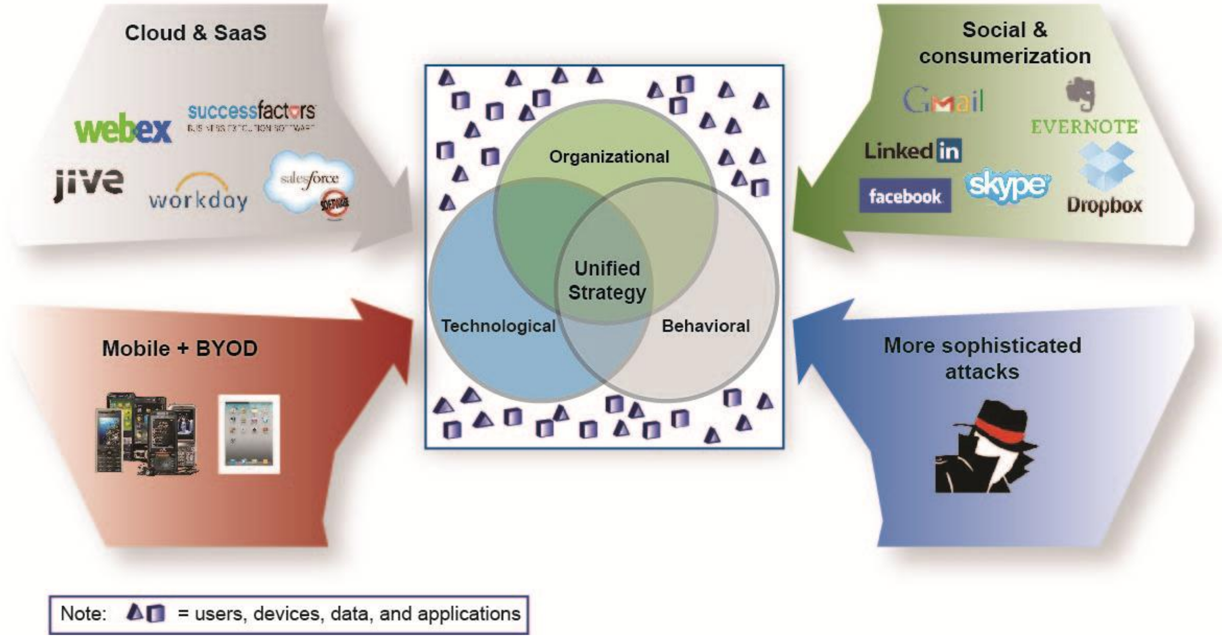


Figure 4: The Three Essential Elements to Create a Unified Strategy

3.0 CURRENT GOVERNMENT ENVIRONMENT

Threat actors to Federal information systems and systems supporting critical infrastructure constantly compete with efforts to stop them. This section describes the current information system and threat environment, as well as specific Government programs and initiatives designed as countermeasures.

3.1 Threat Environment

Cloud computing, bring-your-own-device (BYOD) practices, and social media trends have introduced thousands of applications, threats, and vulnerabilities into Federal networks, which are increasingly hidden from traditional network security devices. This can lead to advanced attacks (e.g. APT), wherein malicious actors use comprehensive network reconnaissance to navigate a victim's network faster and more effectively. Once inside a network, advanced attackers can execute a series of actions to entrench themselves and compromise systems. These actors typically attack very strategic targets and will continue to do so until their mission is complete.

What Has Changed?
Cyber attacks on the Federal Government have increased in frequency, agility, persistence, sophistication, complexity, and covertness.

The current threat environment is depicted in a variety of industry and Government reports. For example, a recent in-depth survey of enterprise network managers found that two-thirds of all data breaches in 2012 went undiscovered a month or longer, and another cybersecurity report found that the typical advanced attack goes unnoticed for nearly eight months.[12,13] The current cyber threat environment is also discussed in the *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act* (FISMA) *of 2002*, which acknowledges that APT is a significant threat to Federal information systems.[14] The report states that systems' defensive security posture is "a constantly moving target, shifting due to a relentless, dynamic-threat environment, emerging technologies, and new vulnerabilities." It acknowledges that employee telecommuting and remote system access will require organizations to address unauthorized access and personal identification by following NIST guidance for the enablement of authentication services for mobile devices. The report further cites the need to protect against social engineering, insider attacks, and phishing, which make up a large percentage of attacks against Federal networks.

3.2 Elements of the Government's Current Electronic Communications Strategy

The Government currently addresses and implements several technological, behavioral, and organizational solutions, outlined in the following sections, to help secure Federal Government communications. The NSTAC recognizes these efforts and used them as a baseline upon which to present additional novel approaches and recommendations for the Government's consideration.

[12] Verizon Communications, Inc. *2013 Data Breach Investigations Report*. Available: http://www.verizonenterprise.com/DBIR/2013/.

[13] Mandiant Corporation. *M-Trends 2013 – Annual Threat Report on Advanced Targeted Attacks.* Available: www.mandiant.com/mtrends2013.

[14] Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

3.2.1 Technology

What Has Changed?
The new technologies, such as cloud computing and mobile, remote access by tablets or smart phones, all reside outside the Federal enterprise perimeter.

As previously noted, emerging technologies and new vulnerabilities complicate the dynamic threat environment facing our Nation today, as many of these technologies operate outside the Federal enterprise perimeter. As the department responsible for securing civilian Government networks, the Department of Homeland Security (DHS) has allocated funding to support a variety of programs to mitigate the new threat environment and ensure essential public services.[15] These programs include:[16]

- **Trusted Internet Connection (TIC) Initiative.** The TIC Initiative aims to consolidate the number of external Federal Government access points (including those to the Internet) to help implement a common security solution across all agency networks.
- **Continuous Diagnostics and Mitigation, Tools, and Continuous Monitoring as a Service Program.** An essential part of the Federal Government's risk management process, this is a collaborative program among DHS, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST) to perform continuous diagnostics and monitoring of D/A information systems to increase cybersecurity situational awareness.[17]
- **Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*.**[18] Overseen by DHS, this directive requires the implementation of personal identity verification (PIV) cards for Federal employees; the cards allow for two-factor authentication to agency networks.[19]
- **EINSTEIN Program.** Developed to help enhance the Nation's cybersecurity situational awareness and incident response capabilities, the EINSTEIN Program is DHS' automated process to collect, correlate, analyze, and share data on cybersecurity threats across the Government.

[15] See Appendix F. Written testimony of Acting Deputy Secretary Rand Beers for a Senate Committee on Appropriations hearing titled "Cybersecurity: Preparing for and responding to the enduring threat." June 12, 2013. Available: http://www.dhs.gov/news/2013/06/12/written-testimony-acting-deputy-secretary-rand-beers-senate-committee-appropriations.

[16] The Office of Management and Budget deems the first three programs top priorities. See: Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

[17] Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

[18] Office of Management and Budget. Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–*Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011. Available: www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.

[19] Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

In addition to programs designed to combat and address threats, the Government is also integrating cloud computing, BYOD practices, and social media into its operations. The policies outlined below have been created to govern the technologies' implementation.

Cloud Computing

To address the Government's migration to cloud computing and the resulting need for security, OMB made cloud computing an integral part of the *25 Point Implementation Plan to Reform Federal Information Technology Management*.[20] Additional elements of the Government's technology solutions include:

- The *Federal Cloud Computing Strategy*, developed to ensure the safety, security, and reliability of data stored in a cloud environment;[21]
- The *Security Authorization of Information Systems in Cloud Computing Environment* policy memorandum, which established FedRAMP, a program that sets forth the roles and responsibilities, implementation timelines, and requirements for D/As; and
- The draft *U.S. Government Cloud Computing Technology Roadmap*, developed "to accelerate Federal agencies' adoption of cloud computing, support the private sector, improve information available to decision makers, and facilitate the continued development of the cloud computing model."[22]

BYOD Practices

Recognizing the migration to mobile devices (including personally-procured devices) by the Federal workforce, NIST has developed several policies and guidelines to help increase mobile device security. In particular, NIST is finalizing the second revision of HSPD-12, and Federal Information Processing Standards Publication 201, *Personal Identity Verification of Federal Employees and Contractors*, to address the integration of PIV credentials with mobile devices and advances in technology.[23] In support of this effort, NIST is also developing Special Publication (SP) 800-157, *Guidelines for Personal Identity Verification-Derived Credentials*, which is expected to be released in late 2013.

NIST has also issued two draft documents to help secure organization-issued and personally-owned devices brought into a Federal organization: (1) SP 800-124 Revision 1, *Guidelines for*

[20] Office of Management and Budget. U.S. Chief Information Officer. *25 Point Implementation Plan To Reform Federal Information Technology Management*. December 9, 2010. Available: http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf.

[21] Office of Management and Budget. U.S. Chief Information Officer. *Federal Cloud Computing Strategy*, February 8, 2011. Available: https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

[22] Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

[23] National Institute of Standards and Technology. Federal Information Processing Standards Publication (FIPS PUB 201-1), "Personal Identity Verification of Federal Employees and Contractors." March 2006. Available: http:// csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf; National Institute of Standards and Technology. See also: FIPS PUB 201-2, "Personal Identity Verification of Federal Employees and Contractors-REVISED DRAFT." July 2012. http:// csrc.nist.gov/publications/drafts/...2/draft_nist-fips-201-2_revised.pdf.

Managing and Securing Mobile Devices in the Enterprise, to help organizations centrally manage and secure mobile devices; and (2) SP 800-164, *Guidelines on Hardware-Rooted Security in Mobile Devices*, to provide a common baseline of security technologies that can be implemented across a wide range of mobile devices.[24]

Social Media

The Federal Government has recognized that social media can provide several unique benefits, including increased citizen engagement and fast and efficient distribution of both regular communications and breaking news. Social media also provides new opportunities for intra-Government collaboration.[25]

The Government acknowledges that there are significant risks to social media interactivity if Federal officials do not closely monitor and manage the increased data flow. The Federal Government has attempted to document and communicate these concerns in numerous reports, including the 2009 Federal CIO Council report, *Guidelines for Secure Use of Social Media by Federal Departments and Agencies*, the 2010 OMB Memorandum 10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, and the General Services Administration's social media policies, which are reviewed and updated regularly.[26]

3.2.2 Behavior

Behavior patterns of the Federal workforce continue to change due to an increase in remote network access; however, the Government lacks an overarching strategy to educate its workforce on risk and consequence management. The Government also lacks a centralized security authority to oversee and implement such a strategy.

What Has Changed?
Evolving human behaviors associated with leveraging the speed and convenience of emerging technologies requires the Government to shift security strategies and train people in different ways.

One Federal program designed to help improve the behaviors related to cybersecurity hygiene is the National Initiative for Cybersecurity Education (NICE). Led by NIST in collaboration with DHS and other Federal D/As, NICE is designed to establish an operational, sustainable, and

[24] National Institute of Standards and Technology. *Special Publication 800-124 (Revision 1) Guidelines for Managing the Security of Mobile Devices in the Enterprise.* June 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf. See also: National Institute of Standards and Technology. *Special Publication 800-164 Guidelines on Hardware Rooted Security in Mobile Devices (DRAFT).* October 31, 2012. Available: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[25] General Services Administration. Using Social Media. Available: http://www.howto.gov/social-media/using-social-media-in-government.

[26] General Services Administration. Social Media Navigator. Available: http://www.gsa.gov/portal/content/250037. See also: The Chief Information Officers Council (2009). Guidelines for Secure Use of Social Media by Federal Departments and Agencies. Version 1.0, September 2009. See also: Office of Management and Budget. Memorandum M-*10-13 Guidance for Agency Use of Third-Party Websites and Applications*. June 25, 2010. Available: www.whitehouse.gov/omb/assets/memoranda_2010/m10-23.pdf.

continually improving cybersecurity education program to improve the cyber behavior, skills, and knowledge of the American population.[27]

Legislatively, FISMA is one of the Nation's most significant Federal network security statues that addresses behavior. FISMA includes a comprehensive risk-based framework to ensure that Federal information security controls are effective; it also requires that D/As develop information security risk reduction policies, including security awareness training for employees.[28] FISMA requires that all Federal D/As perform a risk-based analysis to determine the adequacy of training required (in terms of the amount, content, and frequency) to achieve the appropriate human behavior that can counter today's threats. The *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* also notes that some D/As provide daily or weekly supplemental security training; however, a quantifiable method by which to measure the training effects is not currently in place.

3.2.3 Organization

The Administration directed that the 2008 Comprehensive National Cybersecurity Initiative and its associated activities evolve to become key elements of a broader updated national strategy.[29] In 2009, the Administration released its *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, and the President appointed a Special Assistant and Cybersecurity Coordinator—a significant milestone in advancing a Federal Government cybersecurity strategy.[30] Since the document's release, the Government continues to review and update its Federal cybersecurity policies, evidenced by the 2013 release of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, and Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*.[31,32]

What Has Changed?
FISMA's mandate is IT focused, but the risk to information security is now much greater in scope than technology, thereby creating a growing gap between risk and mission enablement.

Aside from these overarching policy guidelines, the Federal Government's cybersecurity strategy remains largely developed and implemented by individual D/As pursuant to their own unique risk management approaches. Requirements for securing the Federal Government's information systems are addressed in various Federal laws and policies applicable to the D/As.

[27] The four components of NICE are: (1) National Cybersecurity Awareness; (2) Formal Cybersecurity Education; (3) Cybersecurity Workforce Structure; and (4) Cybersecurity Workforce Training and Professional Development

[28] P.L. 107-347, *E-Government Act of 2002*. Title III. December 17, 2002. 44 U.S.C. 3541, et seq.

[29] Executive Office of the President. National Security Presidential Directive 54/Homeland Security Presidential Directive 23: *Comprehensive National Cybersecurity Initiative*. January 2008. Available: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

[30] Executive Office of the President. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. May 2009. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[31] Executive Office of the President. EO 13636, *Improving Critical Infrastructure Cybersecurity*. February 19, 2013. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[32] Executive Office of the President. PPD-21, *Critical Infrastructure Security and Resilience*. February 19, 2013. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

As previously discussed, the most significant law is FISMA, which requires each Federal D/A to develop and implement a security regime to support its IT assets.[33] FISMA's provisions, however, are specifically IT-focused and do not acknowledge or address the larger range of risks within the entire Federal Government enterprise. In addition to training requirements noted in Section 3.2.2, mandated FISMA programs include periodic assessments of the risk of unauthorized, malicious use of information systems, as well as periodic evaluation and testing of IT programs and policies. It is important to note that FISMA's reporting requirements have evolved into a compliance management framework and, collectively, D/As do not have a real-time reporting system. Based on the range of threats, the Federal Government is attempting to focus its attention on the most cost effective and efficient information security controls relevant to each organization.

3.2.3.1 Risk and Consequence Management at the Federal Level

While the Government's ultimate goal is to protect Federal D/As against cyber incidents to the greatest extent possible, officials should also assume and accept that malware exists, and will continue to exist, in today's networks. The Government is beginning to develop tools to manage risk; however, these efforts are currently insufficient due to inconsistent security practices within Federal D/As and the lack of an integrated approach among those organizations.

The *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* describes numerous risk management efforts undertaken across Federal D/As to provide security and deterrence against a terrorist cyber incident. Despite these efforts, Federal D/As in 2012 collectively spent only five percent of their budgets on security tools and only three percent on risk management.[34] Additionally, the risk management efforts described in the report are focused on information security specifically, and not on an aggregated risk management approach. The report also cited that while 18 of the 24 surveyed D/As had existing information security risk management programs, only two had a complete program as directed. Additional significant deficiencies include:

- Ten D/As did not address risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy, as required by NIST SP 800-37, Revision 1.
- Nine D/As did not address risk from a mission and business process perspective and were not guided by risk decisions made at the organizational level, as required by NIST SP 800-37, Revision 1.

Additionally, the *Fiscal Year 2012 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002* does not cite any follow-up actions for D/As that have not achieved a 100 percent rating.

[33] Under FISMA, OMB is responsible for overseeing agency information security policies and practices, and NIST is responsible for prescribing standards and guidelines pertaining to Federal information systems. See: National Institute of Standards and Technology. FISMA Overview. Available: http://csrc.nist.gov/groups/SMA/fisma/overview.html.

[34] Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

One area where the Government has made progress is in NIST's development of a six-step Risk Management Framework. Based on a security lifecycle, this has been adopted by D/As as a framework to address threats against their networks (see Figure 5).[35] Under the framework, D/A systems are tested by tools and tactics associated with malicious agents to determine information security vulnerabilities. Also, security test and evaluation teams provide remediation recommendations to mitigate the vulnerabilities identified.

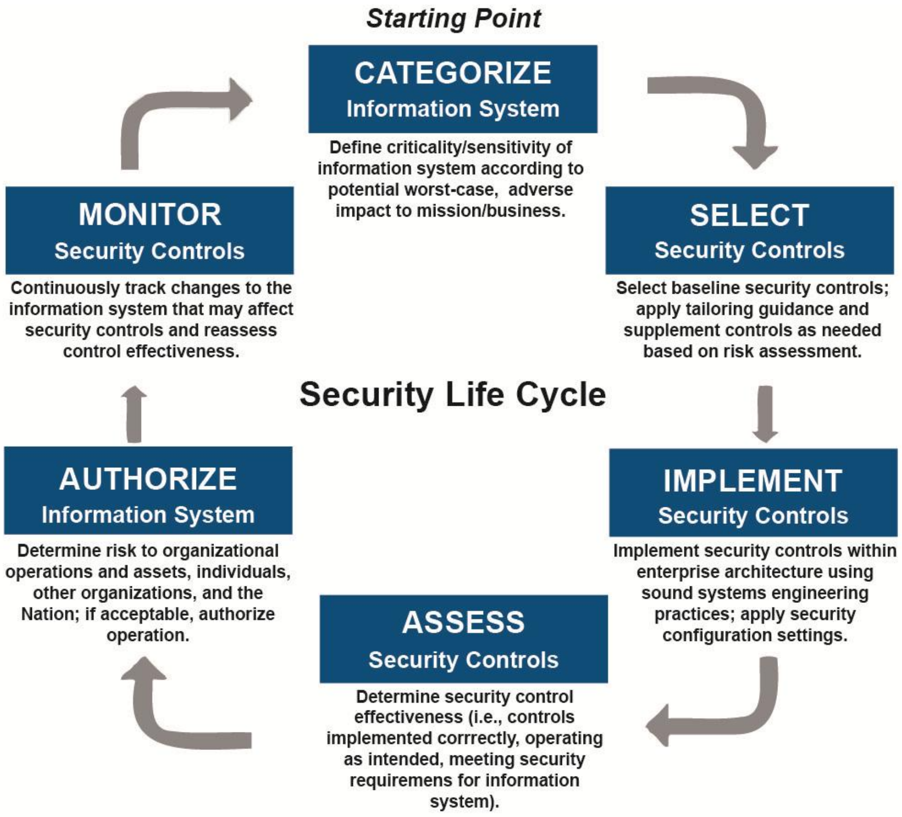

Starting Point
CATEGORIZE
Information System
Define criticality/sensitivity of information system according to potential worst-case, adverse impact to mission/business.
SELECT
Security Controls
Select baseline security controls; apply tailoring guidance and supplement controls as needed based on risk assessment.
IMPLEMENT
Security Controls
Implement security controls within enterprise architecture using sound systems engineering practices; apply security configuration settings.
ASSESS
Security Controls
Determine security control effectiveness (i.e., controls implemented corrrectly, operating as intended, meeting security requiremens for information system).
AUTHORIZE
Information System
Determine risk to organizational operations and assets, individuals, other organizations, and the Nation; if acceptable, authorize operation.
MONITOR
Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness.
Security Life Cycle

Figure 5: NIST Risk Management Framework[36]

Regarding consequence management, the Federal Emergency Management Agency's (FEMA) document, *Managing the Emergency Consequences of Terrorist Incidents*, can serve as a template for other D/As developing a consequence management plan.[37] Though FEMA created this document in the aftermath of the terrorist attacks of September 11, 2001, several points remain applicable today. The report states:

[35] National Institute of Standards and Technology. Special Publication, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Chapter 3.

[36] National Institute of Standards and Technology. Special Publication, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. Chapter 3.

[37] Federal Emergency Management Agency. "Interim Planning Guide for State and Local Governments." July 2002. Available: https://www.fema.gov/pdf/plan/managingemerconseq.pdf. For an additional consequence management plan, see: FEMA.*Contingency and Consequence Management Planning for Year 2000 Conversion: A Guide for State and Local Emergency Managers*. Available: http://www.fema.gov/y2k/ccmp.htm.

Given the creativity of those committed to carrying out acts of terrorism, planners are being challenged to "think outside the box"—to plan for responding to the unimaginable. This guide responds by asking planners to consider a broad range of terrorist incidents, including assaults on infrastructure and electronic information systems that could result in consequences affecting human life, health, and safety.

4.0 COMPONENTS OF THE SOLUTION

What Has Changed?
There is no single technology able to support the volumes of data, the proliferation of applications, or the mobile identity management needed to manage a data environment without a perimeter. Securing government communications now requires concurrent implementation of technological, behavioral, and organizational solutions.

As previously noted, each element of a unified Government communications strategy–technological, behavioral, and organizational–has an essential role in addressing a specific subset of security challenges (see Figure 6):

- Technologically, a more dispersed enterprise means that data is more often in transit to/from, and resident on, a greater variety of devices; further, this abstract data perimeter broadens the surface that the Government must protect.
- Behaviorally, a more mobile workforce means the usage of additional computing platforms, many of them personally-procured and managed; the lack of appropriate user training can have cascading impacts.
- Organizationally, dispersed authority for cybersecurity can yield inconsistent compliance, uneven implementation of responses, and diluted accountability for real-time, long-term security standards and processes.

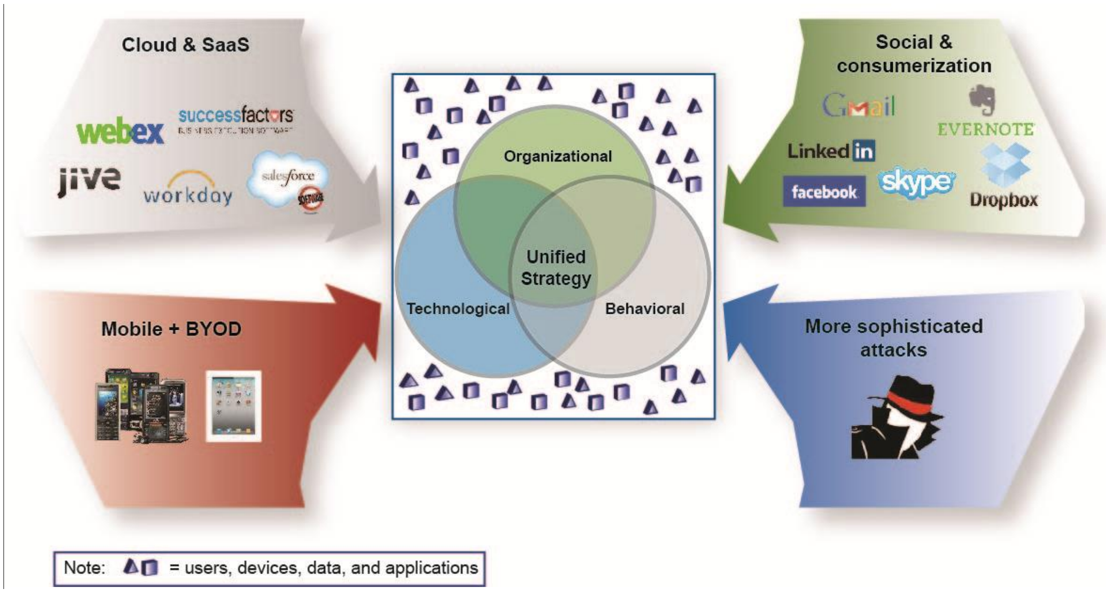


Figure 6: The Three Essential Elements to Create a Unified Strategy

The private sector faces similar challenges and threats regarding the security of its data and communications, and has implemented many novel approaches to enhance information security. In today's threat environment, these measures have been found to be both essential and effective; adoption of a balanced and holistic program of technological modernization, behavioral reinforcement, and organizational adaptation to maximize results and manage processes are no longer optional. The approach of a combined technological, behavioral, and organizational solution should be considered and evaluated by the Federal Government for implementation. The components of the approach (i.e., technology, behavior, and organization) will be discussed in the remainder of the section.

4.1 Technological Solutions: Establishing New Cybersecurity Strategies

As users increasingly embrace devices with remote access capabilities, cloud technology, and social media, the Federal IT enterprise's total volume of data continues to increase. Today, access to and exploitation of data applications represents the primary path for malware entry into networks.[38] This problem is exacerbated by the current lack of central authority and operational control of Federal Government data and systems.

What Has Changed?
Since 2007, revolutionary technological advances include the rapid adoption of shared, dispersed cloud computing capabilities; mobile computing devices and smart phones; growing connectedness through social media; and system interdependencies causing consequences across infrastructures.

The need for a new, next generation network (NGN) security approach across the Government can no longer be disregarded.[39] The next generation of network security practices must not only be able to see, but also classify, all network traffic in an integrated, multi-functional process, with granular controls. When implemented properly, an NGN security approach will facilitate adoption of modern technologies and implementation of enhanced security policies and processes, enabling advanced functionality and flexibility for the D/A user.

The following subsections of Section 4.1 comprise several technological advancements that may be beneficial and effective to securing Government information systems. While security experts could argue that these approaches alone are not novel, when combined, these practices form the basis of cybersecurity and risk regimes implemented by many corporations under current conditions.

[38] Microsoft. "Microsoft Security Intelligence Report." Volume 11.Available: http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf. See also: NSTAC SGC Briefing. Mykonos Software. January 22, 2013.

[39] The basic functional description of next generation network security generally includes: (1) identification of applications, regardless of port, protocol, SSL or threat efforts to evade such understanding; (2) user identification, regardless of claimed IP address; (3) device authentication, known people should be accessing systems from known devices; (4) real-time protection against threats; (5) policy visibility into and control over the entire network and especially applications; and (6) preservation and enhancement of network performance while achieving all of the above.

4.1.1 Network Perimeters and Data-Centric Approach to Security

Over the past three decades, the primary method of corporate computer security has been focused on establishing rigid and inflexible organizational network perimeters. The enterprise data residing inside the perimeter was once secure because administrators were able to control perimeter security and ensure trusted operations due to a limited number of access points and methods (see Figure 7).

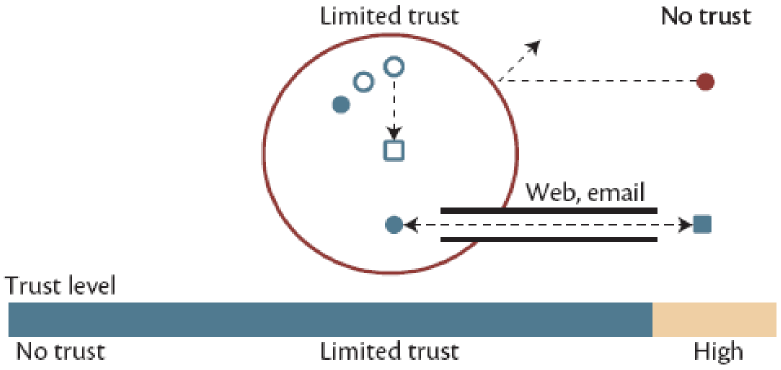


Figure 7: Old Network Perimeter Model[40]

Unfortunately, the old network perimeter model is rapidly losing its effectiveness. Companies now recognize that remote workers need access to organizational data anytime, anywhere, and from any device. As a result, IT departments have created full-time virtual private network access to safeguard corporate assets, including sensitive company data, from any employee device or Web browser. Additionally, cloud offerings allow corporations to virtualize infrastructure (through infrastructure-as-a-service), software (through software-as-a-service), and other business functions. Both of these advancements involve moving the enterprise’s information outside the traditional perimeter defenses and, as a result, the notion of a secure corporate perimeter is becoming obsolete (see Figure 8). This becomes problematic when the same device that has downloaded a questionably-coded application is simultaneously accessing critical corporate resources. With nearly unfettered access to these resources, threat actors have exploited the trustworthiness of the web of enterprise and service provider relationships to exfiltrate significant intellectual property.

[40] Amoroso, Edward G. “From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud.” *IEEE Computer and Reliability Societies*. January/February 2013, Vol.11, No.1. ISSN: 1540-7993.

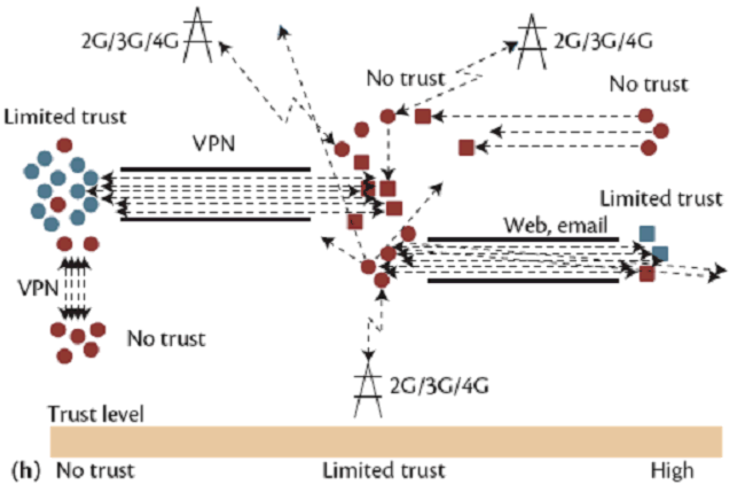


Figure 8: Current Network Perimeter Challenge[41]

In today's evolving threat landscape, the classic concept of fixed and hardened protective barriers surrounding secure domains is no longer viable or defensible; instead, classic security approaches may hamper functionality and efficiency more than their protective value justifies. As data often resides outside of an organization's intranet, data centric security must become the core of the Government's new security strategy. A data-centric approach can be likened to a series of protective rings around data objects (e.g., an email, health care record, or tax document). Some of those rings will travel with the data as it moves from system to system, while others are part of the system hosting the data.

Context-Aware Adaptive Security

Context-aware adaptive security measures allow networks to better respond to threats in today's dynamic, virtualized environment. Context-aware security is defined as "the use of supplemental information to improve security decisions at the time decisions are made, resulting in more accurate decisions capable of supporting dynamic IT-environments."[42] Context information relevant to IT security includes environmental context, application awareness, identity awareness, content awareness, role awareness, and other access data.

All information security infrastructure (including endpoint protection platforms, access control systems, network firewalls, intrusion detection systems, security information, event management systems, secure Web gateways, secure email gateways, and data loss prevention systems) must become context-aware. New levels of large-scale data can yield real-time awareness of: (1) users of data (identity management [IdM]); (2) sources of access requests (device management); and (3) the data being accessed (information rights management).

[41] Amoroso, Edward G. "From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud." *IEEE Computer and Reliability Societies*. January/February 2013, Vol.11, No.1. ISSN: 1540-7993.
[42] Gartner. "Context-Aware Security." Available: http://www.gartner.com/it-glossary/context-aware-security.

Data Loss/Leak Prevention

Data loss/leak prevention (DLP) is an essential element for any data-centric approach to secure communications; in a recent survey, DLP was second only to IdM as the greatest need of IT professionals.[43] Examples of critical and confidential data types (requiring DLP program protection) common to both private sector and Government enterprises include intellectual property (e.g., source code, process documentation, or scientific findings), corporate or organizational data (e.g., legal or financial documents, strategic planning reports, or employee information), and customer or citizen data (e.g., Social Security numbers, credit card numbers, medical records, or financial statements).[44]

DLP programs can be implemented at many levels or locations within a communications security strategy, including:

- Network DLP (data-in-motion DLP), which analyzes network traffic to detect critical data being accessed or forwarded in violation of assigned digital rights or information security policies;
- Endpoint DLP, which runs on end-user systems, such as work stations, and can manage internal and external communications, such as email and instant messaging; and
- File-level DLP, which identifies sensitive files and incorporates the digital rights, information security limitations, or distribution parameters within the file itself so the protections stay with the file whether it is downloaded, copied, or distributed.

Information rights management is the foundational concept of preventing unauthorized access of sensitive information, whether the files are at-rest or in-motion. This program can encrypt files; limit or restrict information that can be copied or pasted; conduct real-time changes in authorized user lists; and track and map all access, usage, or alteration of key files.

4.1.1.1 Novel Defense-in-Depth Techniques

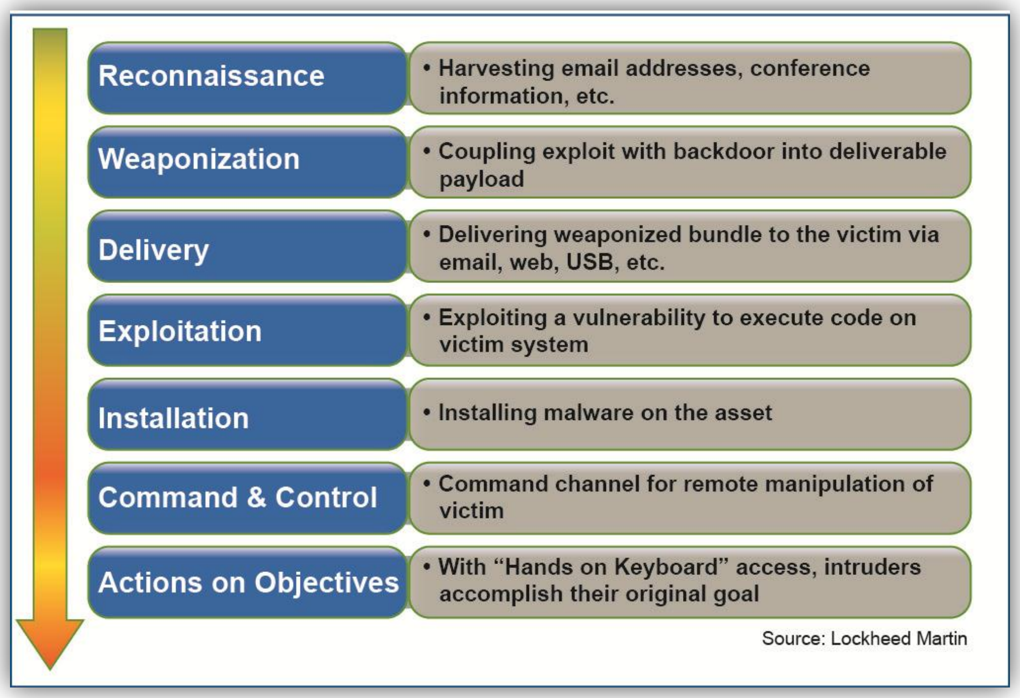
Contemporary defensive approaches presuppose that an adversary has an advantage by knowing the details of a planned attack; however, this advantage is not inherent. Organizations can stop—or significantly reduce the chances of—intruders from achieving their goals by understanding how they operate and adjusting defenses to block their avenues of attack. By leveraging intelligence, expertise, and coordination, organizations can mount an effective defense-in-depth strategy and significantly reduce the success rate of malicious actors. The foundational components of a defense-in-depth approach consists of the following: (1) situational awareness (e.g., security intelligence center, fused intelligence, community information sharing); (2) advanced detections (e.g., custom tools, full packet capture, integrated logging & monitoring, attack replay capability) for both the perimeter (e.g., ingress and egress points that can identify, log, and shun connections) and host (e.g., intrusion detection, group policy, least-privilege); (3) increased agility (e.g., agile organization, operations and on-demand

[43] Messmer, Ellen. "Identity management top security priority in Gartner survey; Data-loss prevention ranks second on the list." *Network World*. June 10, 2010. Available: http://www.networkworld.com/news/2010/061010-gartner-security-identity-management.html.
[44] Veracode. *Data Loss Prevention Guide*. Available: http://www.veracode.com.

response); and (4) risk-based mitigations (e.g., use case dependent, in- and out-bound mitigations, employee awareness, and behavior).

Manual security techniques and processes are insufficient to handle the magnitude of the threat. The speed of response and recovery is essential and can occur only when time-consuming manual operator actions are removed. This means that organizations must introduce autonomic recovery, machine-to-machine interactions that can respond to the threat at the speed that the intrusions are occurring. U.S. industry already has many of the tools and processes required for defense-in-depth strategies. To increase adoption and success of those strategies, U.S. industry is rapidly training a workforce as well as developing new technologies and procedures to close the remaining gaps. The next step is for the cybersecurity community to leverage its emerging understanding of attackers' techniques, tactics, and procedures to apply a defense-in-depth approach to operations.

Advanced tradecraft and proactive services are also needed to address both known and unknown threats, including vulnerability scanning; network traffic and host process anomaly detection; employee human factor mitigation; and developing a comprehensive response practice for cyber attacks. A phased attack methodology, such as a security kill chain, provides a framework for a new security defense strategy (see Figure 9). The defender can achieve strategic advantage by mitigating all phases of the kill chain; the adversaries would then have to change their methodology for every kill chain phase to be successful.



Reconnaissance	• Harvesting email addresses, conference information, etc.
Weaponization	• Coupling exploit with backdoor into deliverable payload
Delivery	• Delivering weaponized bundle to the victim via email, web, USB, etc.
Exploitation	• Exploiting a vulnerability to execute code on victim system
Installation	• Installing malware on the asset
Command & Control	• Command channel for remote manipulation of victim
Actions on Objectives	• With "Hands on Keyboard" access, intruders accomplish their original goal

Source: Lockheed Martin

Figure 9: Sample Security Kill Chain

The security kill chain can dramatically reduce successful attacks; however, a strategy for ensuring resilient systems must also address the eventuality that, no matter how well defended, a system remains vulnerable to unknown future attacks, and may at some point be victimized by a successful attack. To reach the ultimate level of effectiveness, solutions must ensure mission resiliency, even during and immediately after an intrusion.

The following subsections describe specific technologies that could comprise a defense-in-depth strategy.

4.1.1.1.1 Containerization/Enclaving Data

Historically, containerization has been used in regards to device management, wherein a generally untrusted device (e.g., a personally-procured device used for business functions) may have a more-secure "container" installed within it to encapsulate data. Since these containers are intended for known and trusted users to access networks, a higher degree of trust and security may be expected and maintained when they are utilized. In the context of modern security technology and practice, containers may exist for data, devices, users, and applications, all within and across the geographically-distributed and discontinuous network.

Containerization technologies are used throughout the private sector to create trusted workspaces. Trusted containers can be established at multiple levels within the information infrastructure, from the data elements themselves, to the enterprise networks and cloud processing environments where information elements are created, transformed, and stored. Containers can also:

- Establish communities of people, using technologies like federated IdM;
- Establish compartments within computers and personal devices to separate work environments from personal tasks, as well as separate higher or unknown risk activities from preauthorized activities; and
- Allow organizations to establish communities of trusted systems and applications using technologies like whitelisting (see Section 4.1.1.1.2) and reputation-based services.

Organizations apply containerization with the presumption that some component of a security regime will fail, a breach may occur, and other elements of the system will need to contain the risk and ensure continuity of operations (COOP). Figure 10 illustrates how containers in a mobile device can protect one part of the device from malicious elements located in another part. It also illustrates how information rights management protects data when replicated outside a data center container.

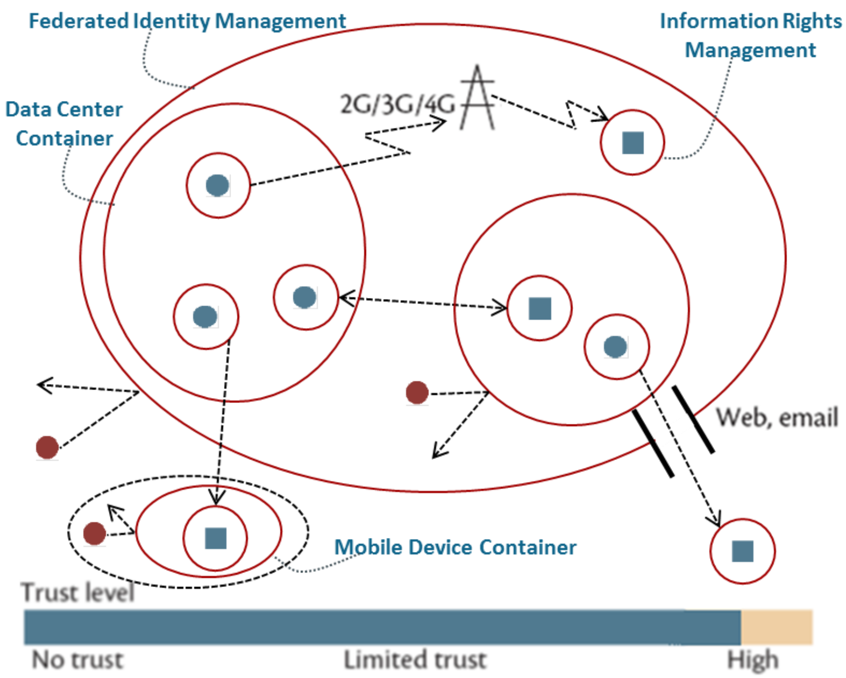


Figure 10: Containerization

The most popular approaches to containerization have been in the mobile device space. For example, by placing a corporate email application in a container, the application remains isolated and insulated against any actions taking place on unregulated portions of the operating system. Another type of mobile device container creates an encrypted processing environment to house sensitive business data and applications. Tools like these allow employees to choose their devices and applications, while IT administrators retain granular control over the business services running in the device. Additional mobile device container options include:

- Enclosing each application—not just data—in its own unique container ("application wrapping"); instead of broadly classifying mobile utilities as either personal or mission-critical, an organization's IT team can tailor custom policies to account for all the notable variations in its enterprise applications.
- Using hypervisors to effectively create a virtual phone within a phone, thereby allowing companies to split an employee device into two isolated segments for personal and work use.

Despite the benefits associated with containerization, containers often rely on device and operating system protections and cannot fully protect data if the device and operating system are compromised by malicious software, a serious consideration in the BYOD environment. For this reason, the scope of security management efforts related to Federal networks should include strategies capable of protecting all users and devices as well as data and applications.

4.1.1.1.2 Whitelisting and Blacklisting

List management seeks to identify unknown sites, users, and applications and determines the threats associated with them. One type of list management, whitelisting inhibits uncontrolled access to malicious applications, sites, and users by establishing a list of "known-to-be good" and authorized entities. Blacklisting uses a list of "known-to-be-bad" and unauthorized entities, such as Web sites with malware or malicious applications. While blacklisting is a good practice, attacks from new sources can still penetrate networks via historically-trusted users, ports, and protocols; therefore, presumptions about trusted users, content, or applications should not be considered infallible.

In today's open network environment, no user, device, or data can be truly and permanently trusted. As a result, organizations and behaviors must be adapted to achieve greater visibility and control. By permitting unknown users and/or devices to access networks, while maintaining full and continuous monitoring of their behavior, security managers will have the best chance of quickly identifying malicious actors and attackers and permit authorized users the maximum flexibility to meet their changing operational needs. Application of these principles maximizes the ability of network managers to achieve and maintain broad visibility over and control of the entire extended-network enterprise. Ways to achieve this outcome is discussed in greater detail in Sections 4.2 and 4.3.

4.1.1.1.3 Trusted Computing Platforms

Trusted computing typically describes an environment in which computers consistently behave in expected ways. Behaviors are defined by computer-based policy and enforced by hardware-based "roots of trust" at the edge of the network and at the endpoint devices to provide higher assurance that devices are operating as intended, and producing the desired outcome with respect to security.[45,46] Trusted computing platforms can help improve the security of Government communications by improving transaction authentication, hardware and software integrity, data protection, network access and identify in on premise, cloud, and mobile computing environments. These platforms should be used in conjunction with a risk management strategy to meet the risk posture for critical assets.

Trusted computing platforms use widely-accepted specifications, allowing any user to integrate the technologies into their products, whether they are based on proprietary or open source designs. The technologies most applicable to securing Government communications include the

[45] This root of trust is established by loading hardware with a unique encryption key inaccessible to the rest of the system.

[46] Trusted computing platforms are based on a set of open, global industry standards and interoperable technologies. The Trusted Computing Group (TCG) is a not-for-profit organization that develops and defines the standards that support a hardware-based roots of trust. TCG has more than 130 members, including for-profit, non-profit, and government organizations from around the world. Over the last ten years, TCG and its members have developed dozens of standards that have been implemented in thousands of products and adopted by international standards organizations, including ISO and IETF. To date, almost two billion endpoints have been secured using trust computing standards. See: http://www.trustedcomputinggroup.org.

trusted platform module (TPM), self-encrypting drives (SED), and trusted network connect (TNC).[47,48,49]

Trusted computing platforms can also help improve the security of mobile devices, especially given increased BYOD practices. Many of today's devices contain unencrypted, confidential data; if stolen, mobile devices may pose a sizable risk to Government functions and the individual information stored on these devices. Adding SED technologies to mobile devices can significantly reduce the risk of data breach, malware, unauthorized network access, and other security challenges. Enterprises also use existing TNC standards to ensure that guest workers, contractors, and remote staff can safely and securely connect to the corporate network.

Trusted computing platforms are already in use today across a wide range of Federal D/As, as well as critical infrastructure sectors. In 2007, the Department of Defense (DOD) issued a requirement that all new computer assets procured to support DOD include a TPM.[50] TPM and SED technologies are relatively cost effective and widely available in computers and servers today. Software and hardware manufacturers are also finding new ways to leverage TPM to improve overall information security and protect data at-rest or in-transit. In fact, the Forrester Research report, *Best Practices: Server Operating System Security*, recommends that enterprises adopt servers containing a TPM to process all high-value transactions.[51]

4.1.1.1.4 Research/Deception Networks

To detect and thwart motivated attackers, organizations must look beyond traditional signature-based detection and vendor-supplied signature feeds; instead, organizations should acquire attack indicators from deception networks, analyze prior attack events, and increase information sharing. Using these types of attack mitigation defense techniques, organizations can make attack execution significantly more difficult or even unsuccessful since an adversary's techniques, tactics, and procedures (TTP) are known by the organization's network defenders. Additionally, an organization may even use its knowledge of the adversaries' tactics to collect additional information about attackers and their methods by constructing artificial resources in which attackers may attempt to infiltrate.

[47] TPM is a hardware module that supports secure key storage, cryptographic functions, and integrity measurement. These capabilities enable strong user and device authentication, secure storage, and hardware-based verification of firmware and software integrity.

[48] SEDs enable integrated encryption and access control within the protected hardware of the drive. They provide the industry's preferred solution for full disk encryption, protecting data when the machines or drives are lost or stolen, as well as re-purposed, require warranty repair, and are at end-of-life. SEDs can be completely and securely erased by simply sending a properly authorized command telling the drive to generate a new encryption key, a much more efficient and effective technique than degaussing or physically destroying the device. Open standards provide multivendor interoperability, allowing application vendors to provide management for multiple SED providers.

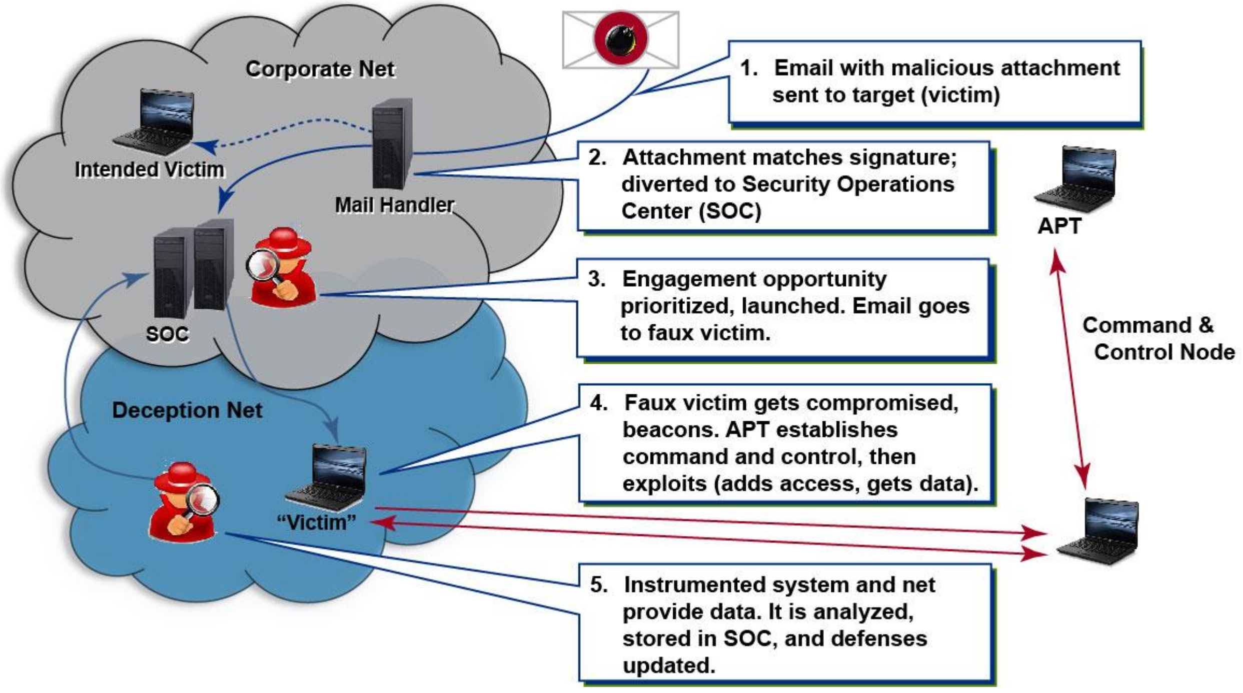
[49] TNC standards are designed to enable various network security functions, including support for endpoint assessment with continuous monitoring, network access control, and security automation.

[50] Department of Defense. "Encryption of Sensitive Unclassified Data at Rest on Mobile computing Devices and Removable Storage Media." July 3, 2007. Available: http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf .

[51] Mulligan, Jennifer Albornoz. "Best Practices: Server Operating System Security." *Forrester*. July 12, 2007.

One example of an artificial resource is a honeypot, a simulated system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to attract potential hackers and intruders and has no authorized users other than its administrators.[52] A second resource is a honeynet, also known as a research or deception network, which can provide defenders with additional information to further protect the organization's resources. Although leveraging research/deception networks and servers to obtain TTP can be useful, it can be difficult to convince attackers that they have successfully infiltrated a targeted enterprise network.

Research/deception networks and services are far more useful than mere public-facing honeypots often targeted by adversaries (see Figure 11). Attack indicators may be entered into research/deception networks to provide additional attack detection indicators when executed, as the attacker intended. Allowing the adversaries' reconnaissance and exploits to run in a controlled environment allows security researchers to provide an organization's security personnel additional indicators that would not have been gathered by blocking initial attack attempts. Additional indicators acquired could include command-and-control server locations, covert communication channels, additional malware downloads, or even direct exploitation by and interaction with an adversary. Indicators may then be entered into a production network's defenses to provide further detection capability. Overall, any of these acquired indicators can help an organization identify future attacks by shifting the kill chain to favor the organization, thereby decreasing the likelihood of a successful attack.



1. Email with malicious attachment sent to target (victim)
2. Attachment matches signature; diverted to Security Operations Center (SOC)
3. Engagement opportunity prioritized, launched. Email goes to faux victim.
4. Faux victim gets compromised, beacons. APT establishes command and control, then exploits (adds access, gets data).
5. Instrumented system and net provide data. It is analyzed, stored in SOC, and defenses updated.

Figure 11: Example of a Research/Deception Network

[52] Kissel, Richard (Editor). "Glossary of Information Security Terms." National Institute of Standards and Technology. NISTIR 7298 Revision 2. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

Threat intelligence from research/deception networks can be used to prepare for and prevent future attacks. Employed properly, these networks can be highly effective and also advance reactive approaches for detecting intrusions to proactive approaches.

4.1.1.2 Application Security and Awareness

The explosive proliferation and wide range of IT applications challenge current cybersecurity authorities and efforts within and outside of the Government. Applications are designed to be readily accessible and easily downloadable, as well as provide convenient and/or intriguing functionality to attract users at little or no cost. Since many applications provide appropriate, even necessary, functionality to both Government and commercial users, it is impossible to entirely block access to Web applications without incurring significant productivity penalties. At the same time, unconstrained access to applications practically guarantees the introduction of malware into networks, possibly via unmonitored paths and gateways.

Modern APTs are agile, creative, and determined in using secure socket layer (SSL) encryption, variations of port or protocol, and other evasive tactics to deliver their malware payloads. To help guard against an APT, all Government IT domains need visibility and control of applications brought into the network and accessed from within it. It is possible to divide the applications issue into two major security challenges: control over data being exfiltrated from networks without authorization, and malware being introduced into those same networks. Both of these challenges involve the use and control of applications.

Voice-over-Internet Protocol (VoIP) applications, for example, present a unique problem in regards to unauthorized data exfiltration. Although VoIP applications are designed to provide a direct conduit into and out of a network, their existence creates a significant risk of unauthorized data exfiltration. At the same time, the qualities that make widely-used VoIP applications so convenient to install and operate can also disguise port-hopping techniques that would otherwise evade network protection screening technologies. Instant messaging applications also present a similar profile in that while they are also ubiquitous and conveniently offer direct file transfer functionality, their existence increases the risk of unauthorized data exfiltration. Instant messaging applications are also susceptible to malware and, in this case, the opportunity to hop to an infected user's contact list constitutes the risk of expanded malware penetration.

Unified communications (UC) technologies that converge voice, video, and data applications present another unique problem. UC technologies allow users to access and share information at risk for unauthorized data exfiltration. In addition, UC's real-time communication requirements may make it more vulnerable to malware, denial-of-service (DoS), or distributed denial-of-service (DDoS) attacks because voice and video quality are affected by even minor delays. As a result, session border controllers (SBC) were developed to minimize the threat of unauthorized data exfiltration, malware, or DoS/DDoS attacks. SBCs authenticate and authorize user access as well as secure, rate, limit, and inspect both the UC signaling and media traffic to help minimize the risk of unauthorized data exfiltration and provide a more resilient infrastructure. In addition, SBCs provide additional protections against attacks that are specific to the UC/VoIP infrastructure.[53]

In addition to appearing as widely-deployed, commercial work-enhancement applications, APTs have increasingly disguised recent attacks using custom and/or encrypted applications.[54] These malicious applications include those developed and operated—and therefore recognized as—for internal, proprietary use by unknowing targets. An industry report on application usage reveals that certain popular commercial applications, including those often employed in the course of conducting unclassified Government business, consume a large portion of bandwidth, even though they are generally safe.[55] The report also states that while SSL encryption can provide security protection in some cases, it masks malware delivery in others. These industry report findings underscore that even trusted applications require continuous monitoring, policy oversight, and adaptive controls. As such, adaptive controls may provide varying levels of user access, user class access, or user privileges, while overseeing user behavior on the network at all times. Content must be screened to ensure that it does not serve as a medium to introduce malware.

4.1.2 Centralized Policy, Decentralized Execution

Communications security professionals across various private sector enterprises assert that an organization can adapt to increased user and data mobility as well as growing threats in two ways: (1) centralizing an organization's policy coordination and standards compliance authorities; and (2) expanding the group of an organization's partners and stakeholders to help implement policies and execute compliance. The following subsections describe industry's approach to enhancing communications security and how this approach can be applied to the Government.

4.1.2.1 Prioritized Data Protection Policy

In a study conducted by the Economist Intelligence Unit, researchers asked private sector executives about strategies that have been successful in promoting a data-driven culture; half of the respondents mentioned top-down mandates and guidance (see Figure 12). The importance placed on this issue was even higher among executives from top companies; over two-thirds of whom noted the importance of executive leadership on data issues.

[53] These threats include toll-fraud, phishing, spam-over-IP telephony, war dialing, and other attacks. See Sipera Systems. "Sipera VIPER Lab Reveals VoIP Security Threat Predictions." Available: http://www.sipera.com/news-events/press-releases/sipera-viper-lab-reveals-voip-security-threat-predictions.

[54] Palo Alto Networks. "The Application Usage and Threat Report - An Analysis of Application Usage and Related Threats – Regional Findings." April 2013. Available: www.paloaltonetworks.com/autr.

[55] Palo Alto Networks. "The Application Usage and Threat Report - An Analysis of Application Usage and Related Threats – Regional Findings." April 2013. Available: www.paloaltonetworks.com/autr.

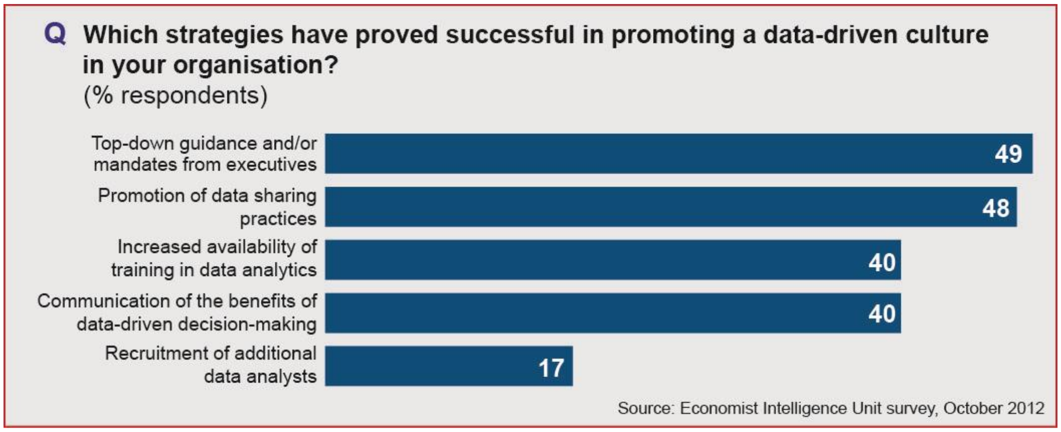


Figure 12: Data-Driven Culture

Clear, consistent, and continuously-enforced prioritized data protection policies are the foundation for a seamless organization-wide, data-centric protection plan. Many organizations have established acceptable Internet use policies. In a similar manner, all relevant stakeholders, including employees, vendors, and customers, should have a clear understanding of how to handle and protect data, including their organization's acceptable access policy. This policy must be implemented using automated mechanisms and enforced across the entire enterprise network, including applications.

Rather than try to protect all data, an organization should prioritize protecting its most valuable and sensitive assets. Doing so will enable an organization to highly restrict and closely monitor access to the specific, dedicated storage or cloud instances where those assets are housed. These cloud instances may include a dedicated mini-perimeter, which is now a viable option due to its limited and controlled access. Additionally, non-critical data and functions should be evaluated for outsourcing to external vendors so that the functions are not directly connected to and cannot directly impact an organization's core network, should one of those functions fall victim to an attack.[56]

4.1.2.2 Identity Management

IdM is critical to ensuring that data access is available to those who require it to support their organization's mission; therefore, IdM should be a key component of any organization's risk management strategy. Organizations must closely attune their broad approaches to IdM policies in order to meet the dynamic needs of operational mission performance.[57] At the same time, more rigorous awareness and linkage of user identity and user actions can help combat insider

[56] An example of such an approach is the Federal Bureau of Investigation's Web portal, which is outsourced to an external vendor and has no direct connectivity with its core internal network.

[57] The NSTAC has long been active in and supportive of Government IdM efforts. The 2009 *NSTAC Report to the President on Identity Management Strategy* explicitly noted that "a comprehensive national vision and strategy for IdM will substantially enhance the overall security and integrity of the national communications infrastructure," promoting operational characteristics including interoperability, trust anchors, choice-based participation. The White House subsequently released the *National Strategy for Trusted Identities in Cyberspace* (NSTIC) in April 2011, which supported the principles of NSTAC's recommendations, including that IdM solutions be privacy-enhancing, voluntary, secure, resilient, interoperable, cost-effective, and easy to use.

threats facing organizations. Insiders remain a constant avenue for data loss; according to a 2012 report, insider threats accounted for 14 percent of reported data breaches and 13 percent of reported privileged data abuse or misuse.[58]

Due to the changing environment, the Government should reexamine its approach to IdM, as well as modify plans and programs to reflect the current state of technology, intended functionality, and threats. Specific modifications should address the following topics:

- **Device IdM:** Autonomous device-to-device communications, sometimes described as the emerging "Internet of things," must be anticipated in the overall IdM and larger cybersecurity ecosystems. Proliferating mobile systems compound IdM issues dramatically.
- **Technology disruption:** Several developments in the IT-based work environment require reexamination of historic governmental approaches to IdM. One example is credential management, with an emphasis on hard tokens. Using public key infrastructure-based encryption methods to secure online sessions (e.g., via SSL) must be reexamined in the face of advancing threats.
- **Evolving trust marks:** The Government should address how trust marks should be administered, the rigor of the certification and maintenance processes, and who decides which trust marks have value in specific environments.[59]
- **Certification of personnel permitted to interact with the systems:** Experienced network users and administrators may lack awareness of ongoing threats, and it may be unclear to what they should pay attention. There is a clear need for greater focus on users and administrators who are authorized to access valuable information or the systems that store, operate on, and protect that information.
- **Identity of content and applications:** In addition to identifiable users and devices, the total federated IdM environment must embrace data content and applications employed within the network. This is achievable and necessary today, due to the demonstrated tendency of the threat to infest otherwise-trusted applications.
- **Environmental complexity:** Today's environment includes many factors involved in securing the systems on which missions or operations depend.[60] APTs appear benign as they move through systems, transported by seemingly innocuous data until they either encounter a trigger or are activated in some other fashion, after which they cause damage and often self-eradicate.

4.1.2.3 Device Management Policy

Control and oversight of employer-issued devices, servers, peripherals, and networking equipment is often overlooked in centralized security policy management. Frequently, these policies are decentralized, uncoordinated across an organization, or not addressed in policy

[58] Verizon Communications, Inc. *2013 Data Breach Investigations Report.* Available: www.verizonenterprise.com/DBIR/2013/.

[59] Trust marks have become a large area of discussion in the *National Strategy for Trusted Identities in Cyberspace*.

[60] For example, central hosting, cloud computing, increasing reliance on mobile systems, layered defenses, smart cards and biometrics are all well into deployment and use.

statements, thereby resulting in a fractured and uncoordinated approach to device management. Because an organization rarely has full technical control over a commercial device's origin and original programming, it is often assumed that a new device or piece of hardware either contains outdated software or is pre-infected with malicious code. A centralized device security policy is imperative in order to permit the use of commercial devices with reasonable risk management.

Local acceptable use policies describe the proper use of a device issued to an employee (i.e., whether or not employees may use an issued device for personal communications). Top-level centralized policies must address device-specific security issues, such as:

- The acquisition process;
- Steps taken after the device has been delivered, but before it is issued to an employee (e.g., installing software updates, removing or deactivating features);
- Installation and management of organization-specific software, which may include tracking software;
- Registration of the device and assignment to an employee's name or identification number;
- Methods for deactivating and wiping the device should it be lost or misused;
- Terms and agreements for the use of privately-owned devices inside organizational buildings and perimeters, especially if they can connect to the organization's networks; and
- Implementing network access control to allow only registered devices through the enforcement of device-level authentication.

A similar centralized hardware security management approach should be taken for servers, peripheral devices, networking equipment, and other hardware devices that are not typically issued to individual employees for their own use, but are purchased from the commercial market.

4.1.3 Large-Scale Data Analytics

Large-scale data analytics refers to the analysis of large volumes of data sets (big data) to find patterns and insights that might not be observable without advanced analytics. This method provides organizations the depth and breadth needed to link disparate information systems to turn billions of events into a few actionable items for analysis. Big data originates from many sources, including the sensors designed to collect climate data, social networking sites, videos and digital images, cell phone Global Positioning System signals, and sale transaction records, among others. In the context of cybersecurity, any system that implements a security layer will generate audit data; the amount generated varies depending on the complexity of that system (e.g., involves multiple roles and users) and the level of audit detail desired. Large-scale data analytics uses specialized algorithms, systems, and processes to review, analyze, and present information illuminating abnormal behaviors in a more meaningful format for organizations.

Large-scale data analytics previously required expensive computing resources; however, the availability of low cost, high capacity storage and high performance processing have paved the way for distributed computing environments, thereby allowing large-scale data analytics to be within reach of most organizations and the Government. More powerful computing and less expensive storage allows terabytes of data to be processed and correlated to provide significantly more accurate identification of potential incidents while reducing false-positives and missing true-positives.

4.1.3.1 Real-Time Context in Cybersecurity

Traditional information systems create many events that overwhelm human capabilities. The goal of data analytics is to provide automation for the association of dissimilar but related events in the mass of billions of events, which organizations must manage on a real-time basis from logs, network traffic, and policy violations. Organizations can then cross-reference these patterns, signatures, and events with cyber threat and business intelligence, which will enable an organization's leaders to understand the positive and negative impacts of this security strategy, the retraining of personnel, and effectiveness of new organizational structures. This technique creates situational awareness of the enterprise and its interdependencies, and it also establishes the health of the enterprise that will change dynamically as the data is processed. When a relationship is identified between information security anomalies, only then can analysts begin to deduce whether a threat is attempting to exploit a vulnerability, or if such an exploit was already successful.

The type of dynamic protections envisioned will require the Government to monitor and manage systems security in real-time. This will permit security authorities to observe and analyze the stream of network activity as it occurs, thereby increasing the ability to rapidly and efficiently: (1) discern how threats evolve; (2) enable security adjustments; and (3) adjudicate user permission requests to access new domains or applications.

4.1.3.2 Active Cyber Defense

Active cyber defense (ACD) describes a range of proactive actions that engage the adversary before and during a cyber incident. It can dramatically improve efforts to prevent, detect, and respond to sophisticated attacks. While ACD is a tactic, it is enabled and accelerated by the development and availability of large-scale data analytics.

As discussed in Section 4.1.1, prior to the recent proliferation of dispersed computing resources and remote, mobile data access systems, enterprises believed perimeter protection was a sufficient defense because they owned their networks, end points, and data. Today, enterprises find it difficult to control access and predict all user behaviors; however, large-scale, real-time data flows and analytics that allow pervasive monitoring of user access and user actions enable enterprises to migrate from a backwards-looking, patch-and-perimeter focus to context-aware, active monitoring, and control of systems' use, data access, and business transactions and requests. Every source of usage data, such as system logs, IdM systems, and asset inventory tracking, can feed this real-time context-aware posture for ongoing data defense.

The changing nature of cyber threats has made ACD increasingly important in both the private and public sectors. Given the effects of today's risk, it is not surprising that both Government and industry are using ACD capabilities to augment their passive cyber defenses. For example, ACD builds on traditional approaches to defending DOD networks and systems, supplementing best practices with new operating concepts. A defense system must operate at network speed by using sensors, software, and intelligence to detect and stop malicious activity before it can affect networks and systems. Intrusions may not always be stopped at the network boundary, so organizations must continue to operate and improve advanced sensors to detect, discover, map, and mitigate malicious activity.

4.2 Behavioral Solutions: Creating a Culture of Security

As technology continues to drive behavioral patterns, organizations need risk and consequence management training more than ever to strengthen their security culture. A key success factor for an effective cybersecurity program is attaining situational awareness and individual accountability for every employee, thereby enhancing enterprise hygiene and guiding program investments and decisions. Cybersecurity training, with a focus on risk and consequence management, provides Government and industry with the situational awareness needed to help reduce threat-related consequences, as well as high returns on investment.[61]

What Has Changed?
The greatest level of success is attained when leadership vision creates a cyber-threat awareness culture that is supported by appropriate behavioral incentives.

4.2.1 Training Programs

Training should target several different communities, all requiring varying levels of awareness to create a culture of cyber threat and risk awareness: (1) executives; (2) mission area leaders; (3) cyber practitioners; and (4) general users, including suppliers and members of the public. When these communities are engaged through tailored cyber awareness programs, they reduce the incidence of malware activation and provide direct benefit to consequence management.

Executives need to understand the cyber threat environment in order to make better risk management decisions, promote the leadership vision for a secure cyber environment, and manage investments and priorities. Throughout its investigation, industry leaders briefing the NSTAC consistently provided measurable outcomes on how the greatest level of success was only attained when leadership vision creates a cyber-threat awareness culture that is supported by appropriate behavioral incentives directly tied to a risk management strategy. [62]

Training for mission area leaders, one of the largest targeted communities, should provide specific information about threats to their programs rather than general threat information. For example, mission area leaders should have the necessary training to determine the following:

- What attacks have been observed targeting the mission program;

[61] "Incentives to the personnel can be in the form of pride, or a competitive nature in which sections of the organizations have higher compliance results than their peers. Displaying the number of phishing attempts to the number of successes by the executive management team to a particular department raises awareness and institutionalizes their actions to be more security focused. Parking places reserved for leadership in security etiquette are well known incentives." Source: SANS Institute. "Methods and Techniques of Implementing a Security Awareness Program." 2002. Available: http://www.sans.org/reading_room/whitepapers/awareness/methods-techniques-implementing-security-awareness-program_417.

[62] For a full list of briefers, see Appendix D.

- What information sets were affected, if any;
- Which users were involved in attacks;
- What open source information is available on the program and its staff (e.g., resumes, affiliations, conference attendance, Facebook™ and LinkedIn™ information, descriptions of assets and weapon systems, key contractors) that may be referenced in social engineering attacks; and
- What information on the program has been retrieved by threat actors from open source locations.

When mission area leaders are involved and provided with specific threat information, they will be able to help identify the assets of greatest concern to them, implement data containerization, determine an estimate of potential damage, and allow the Government to use its resources most efficiently. Mission area leaders also need to understand the threats to their respective mission(s) and the behaviors they need to emulate for their staff.

Cyber practitioners include security operation, security architecture, and engineering professionals and officers. This group needs awareness of emerging threats, changing policies and tools, changing response protocols, and the capabilities of the cyber organization available to assist in cyber defense.

The general user community of Government employees needs to be aware of the threats, as well as develop and routinely implement capabilities to thwart those threats. For employees, these behaviors can be promoted with specific incentives, ranging from mandatory quarterly training, awards for engaging in threat awareness contests, and public acknowledgement of individuals who operated within company guidelines. In addition to Federal employees, suppliers should also receive cybersecurity training. Since suppliers often have access to Government systems and are entrusted with protecting Government information, they need to be aware of the expectations for handling this information and the steps to take in the event of a cyber incident. Finally, citizens also interface with Government systems, accessing and transmitting data containing personally identifiable information that must be protected (e.g., filing Federal taxes online).

The capabilities developed in the user community should include proper information handling and incident response practices. When suspicious events do occur, good cyber training will empower users to take desired actions and involve the cyber organization, which directly reduces an event's consequences. Moreover, a user community that understands the importance of securing Government systems, and does not use Government systems in unofficial ways, will greatly reduce the level of threats introduced to the Government's environment.

An example of a campaign where all users were encouraged to serve as security sentinels was the *If You See Something, Say Something* campaign originally used by the New York City Metropolitan Transit Agency. In 2010, DHS launched the program nationally to promote anti-terrorism and crime prevention awareness across the Nation.[63,64] The Government's messaging to engage as many citizens as possible during the campaign can be adapted for any of the audiences or constituencies interacting with Government communications systems. Finally, security awareness material should be introduced in a variety of formal and informal methods, as employees exposed to the topic more than once will likely retain information better. Formal instruction methods should include security awareness tutorials, training courses, testing, formal presentations of security policies, and professional articles in newsletters. Informal methods should focus on one specific policy and may include newsletter articles, emails, briefings, discussion groups, screen savers, and posters.[65]

By educating their user communities broadly and in the context of their specific work areas, industry has observed decreases in the "click-through" percentage, defined as the portion of users who fall victim to phishing by clicking on a link or opening an email attachment. With increased education, industry's "click-through" percentage fell from an average of 35 percent to approximately 5 percent or lower.[66] To translate this data into consequences, a reduction of 35 percent to 5 percent results in an 85 percent reduction in adversarial success.

4.2.2 Information Security Programs

A best practice information security program with consistent executive management messaging will highlight security priorities and help ensure risks are treated seriously by every employee. Leadership support reinforces executive management's priority to establish each employee as a security sentinel. To ensure that the organization and individual employees are meeting security hygiene goals, management should develop security metrics and consistently review progress against these metrics.

It is necessary for leadership to publicize the security issues, their impacts on the organization, and their relationship to the other interdependencies that the organization is trying to protect. Openly discussing IT governance, risk, compliance, and other topics has many benefits for an organization, including helping: (1) increase the focus on data protection; (2) secure and manage Web 2.0 applications; (3) secure all fixed and mobile endpoints; (4) protect against attacks and evolving threats; (5) secure virtualized and cloud environments; and (6) reduce IT security spending.

The essence of an information security program is the information security controls that protect information confidentiality, integrity and availability. A risk-aware organization would specify,

[63] Department of Homeland Security. *If You See Something, Say Something Campaign*. Available: http://www.dhs.gov/if-you-see-something-say-something-campaign

[64] Secretary Napolitano Announces Expansion of "*If You See Something, Say Something Campaign* to Wal-Mart Stores Across the Nation," Press Office, Department of Homeland Security, December 6, 2010.

[65] SANS Institute. July 2002. Available: www.sans.org

[66] Economics of mass phishing versus spear phishing attacks shows that targeted attacks passing through spam filters have a 35 percent likelihood of click through (70 percent Open Rate x 50 percent Click Through Rate = 35 percent Effective Click Through). Cisco. "Email Attacks: This Time It's Personal." June 2011. Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf. Additionally, defense contractors reported to the NSTAC below percent "click-through" after repeated education, while this public study showed a reduction from 40 percent to 11 percent in a single round of training.

design, implement, operate, and maintain its security controls by assessing the risks, implementing a comprehensive security management framework, and having the organization's leadership publish that framework for the organization. Publishing the measurements of an organization's security hygiene; a service provider's service level agreements (non-sensitive data only); the security improvements implemented; and measurements of success is critical to increasing employees' understanding of the security environment and thereby achieving security accountability. Specific measurement areas are integrity, confidentiality, and availability of communications, as well as the time it takes to identify and mitigate a breach. Once training occurs, an organization should develop a trending report based on this awareness to track progress. Finally, another measurement is aligning the security objectives to the organization's overall objectives and identifying how the objectives have improved product delivery and mission execution.

4.2.3 Information Sharing

Information sharing is one means to help achieve security goals. The NSTAC has long understood and advocated for information sharing in its past studies, most notably in its *NSTAC Cybersecurity Collaboration Report*, which recommended creating a Joint Coordinating Center to improve public-private information sharing.[67] There are two distinct purposes for sharing information: (1) to distribute best practices, which help organizations manage their environments; and (2) to disseminate threat and vulnerability data, which can increase situational awareness and generate successful action. In both cases, continuing education and training on how to capture, manage, preserve, and deliver useful and actionable information to the appropriate recipient directly contribute to the information sharing practices that support a unified strategy to secure Government communications.

Information sharing must also be actionable, either alone or when combined with other information. Often, when only small pieces of information are shared, no resulting action can be taken. A common example is sharing hostile IP addresses without time stamps of when they were observed hostile and the types of actions observed, among others. In this example, the shared information has very little to no value, could be misused, or could create new problems.

4.3 Organizational Solutions: Elevating Risk and Consequence Management

The professional approach to IT has evolved over time. Organizations have generally employed skilled technology specialists to establish, maintain, and secure systems and networks. Organization leaders have generally been highly-experienced practitioners of information technology processes.

What Has Changed?
Given technical and behavioral change, there is now a need for qualitative change in risk management approaches, with consolidation of authority and distributed execution.

At the advent of the IT revolution in the 1990s, these processes were implemented alongside more practiced and traditional means of receiving, transmitting, and storing information in

[67] NSTAC. *Cybersecurity Collaboration Report Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability*. May 21, 2009. Available: https://www.dhs.gov/publication/2009-nstac-publications-0**.**

support of the main work of the enterprise. IT methods were neither mature nor capable enough to be entrusted with the organization's most sensitive data; failure mechanisms were not well understood and senior managers had no personal experience with IT-intensive environments upon which to base trust and confidence. Consequently, the relationship between the role of IT and its management and security was linear and vertical. Low-level technicians reported upward to the leading technology figure of the organization, typically the organization's CIO. This reporting chain generally paralleled the chain of command and responsibility for other managers responsible for various aspects of mission performance. Accordingly, the CIO was a respected organizational leader, but was adjunct to the achievement of other mission functions.

The relationship between IT and management has improved over time. Today, leading industry and Government thinkers have begun to recognize that IT is central to organizational performance. Primary organizational functions are planned for, conducted, and managed via IT systems and processes, to the extent that the loss of full internal or customer-facing IT functionality for even a brief period is a company-threatening event. Accompanying this reality is a broadened understanding of the full set of processes that could cause such risks to continuity and performance. Leading companies are acting on that understanding by evolving organizational structures, as well as the responsibilities and status of those who manage risk, both in IT and throughout the organization. This fundamental shift in orientation of IT security from a vertical process standing alone, to a horizontal one that encompasses other equities and processes represents a qualitative change in the nature of IT security. Following this qualitative change, organizations should evolve the stature, nature, and composition of former IT security units, as well as the title, position, organizational status, and skills required of any such newly-broadened organization's leadership.

Federal D/As' ability to pursue priorities and manage risk as a best practice requires organizational change, which also enhances the talent of personnel needed across the Government. Creating standards, publishing new unified security strategies, and requiring mandatory training could lead to the increased interchange among teams currently managing the infrastructure. This unified strategy lends itself to career building and opportunity, versus the stovepiped approach of multiple tools that are neither integrated nor interconnected with other D/As that already have interdependencies of network systems in place. A stovepiped approach does not lend itself to an information sharing environment or employees' career development.

Economically, having standards and a centralized risk management program will help consolidate efforts across the Government to progress toward several common goals: more secure communications, implementation of a unified strategy across the Government, and establishing security metrics that can be used consistently across D/As. Industry has made this qualitative change, shifting from reacting to unplanned events, such as a computer network break, to proactively managing risk posture. This includes the differentiation and prioritization of data-at-rest and data-in-motion, with a focus on resiliency as well as prevention. With this strategy in place, the Government can develop and deploy consequence management for operational readiness.

4.3.1 Consequence Management

What Has Changed?
Risk reduction is no longer just a function of reducing threats and vulnerabilities. Due to the rapidly changing nature of these two factors in cyberspace, an approach that focuses on consequence management is a more effective and economical approach.

Risk management is often portrayed as a function of threats, vulnerabilities, and consequences, which can be expressed as a simple algebraic relationship:

Risk = Threats x Vulnerabilities x Consequences

In this model, if any of the threats, vulnerabilities, or consequences become zero, then algebraically, risk also becomes zero. Most organizations focus on threat and vulnerability reduction as their methodology for risk reduction or risk management. The concept of managing or reducing the impact or consequence of a harmful event is normally not as high of a priority.

For physical and human risks, an appropriate approach would maximize investments in threat and vulnerability reduction, since both of those factors can often be controlled by the organization; however, in cyberspace, threats and vulnerabilities are frequently beyond an organization's control, which raises the importance of consequence management. While an approach to cyber risk management cannot ignore threats and vulnerabilities, greater emphasis should be placed on factors that an organization can influence, such as the consequences of a harmful event.

Consequence management is typically accomplished via methods used to increase resiliency, such as system or asset redundancy, lowered dependence on other systems, fast recovery times, and infrastructure hardening. This approach might also require a decoupling of infrastructures and services so that if a certain facility or function is disabled (via cyber or other means), its loss will have minimal impact on other facilities or functions that normally depend on it.

In the private sector, consequence management strategies have financial, operational, and organizational benefits. Industry representatives have repeatedly stated that the rapid pace of technological advances and adoption, as well as the concurrent growth in computer system breach attempts, has caused them to increase their focus on anticipating and managing the possible consequences of system breaches. From a homeland security perspective, one former DHS official and current Harvard Kennedy School professor said of this approach, that in addition to "ensuring that fewer bad things happen, the real test is that when they inevitably do, they aren't as bad as they would have been absent the effort."[68] This managerial commitment to resiliency requires as much of a focus on the consequence, including response and recovery, as it does on prevention and detection.

[68] Kayyem, Juliette. "Never Say 'Never Again'; Our foolish obsession with stopping the next attack." *Foreign Policy*, September 11, 2012.

4.3.2 Centralized Risk Management Governance

A centralized risk management governance model would include a position analogous to a Federal senior official for agency risk (see Figure 13). In most private organizations, this position is expressly charged with defining the policy, standards, and processes that organizations use to manage risks related to achieving their mission objectives. Industry has realized many advantages to creating a senior official for risk; an enterprise-wide risk profile can be used by the organization's executive management to support policies and tie an outcome-oriented, organizationally-prioritized strategy.

Instituting this centralized risk management governance framework requires defining and prioritizing the functions and capabilities relevant to the organization's objectives (risks and opportunities), assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress. Industry representatives briefing the NSTAC held that centralizing risk governance allows an organization to more effectively manage all risks to the business/mission (including but not limited to IT risks) and create a strategy for managing consequences of intrusions. By identifying and proactively addressing risks and opportunities, business enterprises protect and create value for their stakeholders, including owners, employees, customers, regulators, and society overall. A holistic risk-based approach to managing an enterprise includes integrating concepts of internal control and strategic planning.

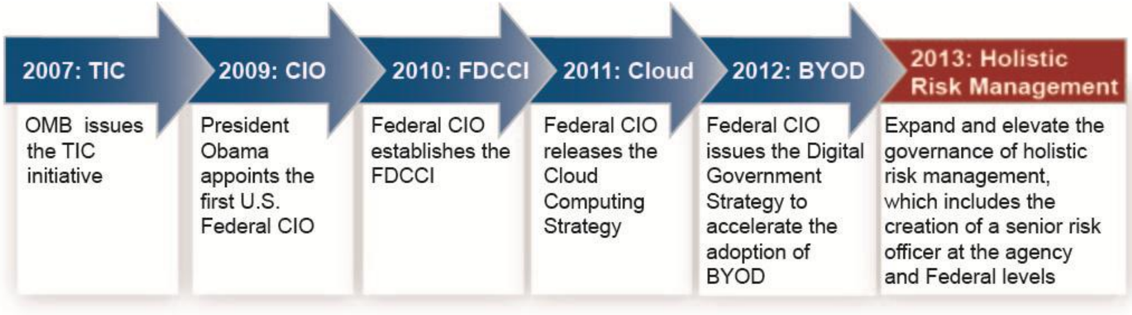

2007: TIC
OMB issues the TIC initiative
2009: CIO
President Obama appoints the first U.S. Federal CIO
2010: FDCCI
Federal CIO establishes the FDCCI
2011: Cloud
Federal CIO releases the Cloud Computing Strategy
2012: BYOD
Federal CIO issues the Digital Government Strategy to accelerate the adoption of BYOD
2013: Holistic Risk Management
Expand and elevate the governance of holistic risk management, which includes the creation of a senior risk officer at the agency and Federal levels

Figure 13: Evolution of Government Initiatives since 2007 with Elevation of Risk Management

Industry leaders and some Government leaders have shifted their organizational responsibilities and made qualitative changes to how they manage enterprise risks. The new paradigm covers all lines of business, creating a shift in strategic emphasis from compliance to improving how security risks are managed. Risks can come from uncertainty in financial markets, project failures, legal liabilities, credit risk, accidents, natural causes, and disasters, as well as deliberate attacks by an adversary. Once organizations expand the alignment of current threats solely from IT to all mission functions, a holistic view of the risks can be addressed.

The best practitioners in private industry have formalized this new paradigm by creating an executive team to oversee risk, specifically creating a risk management board of directors and oversight mechanism to ensure the centralized risk management strategy's effectiveness and integration. This barrier-breaking collaborative mechanism allows management to make a business case for risk analysis and consequence management by sharing insights into strategic planning, anticipated outcomes, and cost of failure from all angles of program management, product development, and future operations. The two essential elements of this approach are: (1) the need for an officially-designated leader of the effort, with complete horizontal convening authority and full vertical access to top management; and (2) inclusive, interactive engagement with a wide variety of stakeholders who manage operational inputs, processes, and outputs.

5.0 LEGAL CONSIDERATIONS

The governing legal authorities for cybersecurity are embedded in multiple Federal statutes and intertwined with Federal policies and directives. Two principal statutes that describe the roles and responsibilities of the Federal D/As for cybersecurity are FISMA (discussed in Section 3) and the *Clinger-Cohen Act*.[69] These two statutes set forth requirements for the procurement and operation of IT systems, the creation of the CIO position, and authorization for the OMB to oversee D/A compliance of cybersecurity requirements. OMB has since assigned its oversight responsibilities under FISMA to DHS in its memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*.[70]

This NSTAC report highlights the need for an overarching and unified cybersecurity strategy across the Federal Government—a position that may be inconsistent with FISMA and *Clinger-Cohen Act* provisions, existing Federal cybersecurity frameworks, Federal D/A CIO and CISO roles, and/or other Federal directives. The current statutory framework makes each D/A CIO responsible for the communications security of that D/A; however, implementation of the NSTAC's recommendations may require a broadening of statutory Federal roles and responsibilities as found in existing laws. This includes risk management to reach beyond information security and remain current with today's COOP policies. For example, it is unclear if some D/As can legally share certain types of information with other D/As—a constraint that could prohibit the Government's adoption of an overarching cybersecurity strategy.

A thorough review of all statutes affecting the Federal cybersecurity posture was beyond the scope of this report. Appendix E identifies several relevant laws that the Government should review.

6.0 FINDINGS

To counter rapidly evolving threats while adopting technological advances, the NSTAC developed multiple findings to help the Government implement a unified strategy to secure its unclassified communications. During its examination, The NSTAC identified three equally-essential and interdependent types of solutions required for a unified strategy, those pertaining to technology, behavior, and organization.[71] Findings specific to each element are categorized accordingly, below.

[69] P.L. 104-106. Clinger-Cohen Act. February 10, 1996. Available: www.fismacenter.com/Clinger%20Cohen.pdf.
[70] OMB released M-10-28 on July 6, 2010.
[71] The parenthetical notation following the each finding refers to the section of the text where the finding is discussed.

Technology:

1. NGN security offers the option to see and classify all network traffic in an integrated, controllable multifunctional process while facilitating adoption of processes offering advanced functionality and flexibility. (Section 4.0) The tenets of the NGN include:
    - Identification of applications regardless of port, protocol, SSL, or efforts to evade such understanding;
    - User identification, regardless of claimed IP address;
    - Real-time protection against threats;
    - Policy visibility into and control over the entire network and especially applications;
    - Continuous monitoring; and
    - Preservation, and ideally enhancement, of network performance while achieving all of the above.
2. Classic, single-function security devices are increasingly unsuited to the needs and opportunities of modern information protection. (Section 4.1.1)
3. Government networks have been slow to embrace multi-functional, NGN security. (Section 4.1.1)
4. A unified security approach to enterprise network security provides a foundation for a clear, consistent, seamless organization-wide implementation of detection, prevention, and remediation. (Section 4.1.1.2)
5. New cybersecurity strategies, which focus on the consequences of impacts to key data (data-centric), have driven industry to adopt new defense-in-depth techniques. (Section 4.1.1.1)
6. Many commercial and Government applications lack the controls necessary to limit access to specified users with the minimum required privileges and lack functionality. (Section 4.1.1.2)
7. Containerization techniques provide a means to isolate functions, as well as monitor, contain, and mitigate the risks to any one element of the infrastructure in the event of a cyber incident. This approach supports a data-centric protection focus where information elements are the primary objects protected. (Section 4.1.1.1.1)
8. Containerization techniques provide an additional defense-in-depth mechanism to mitigate the risks associated with applications and access control, reducing the consequences of an unforeseen breach. (Section 4.1.1.1.1)
9. Organizations rarely have full technical control over commercial devices' origin configuration and factory installed software; therefore, centralized management controls that are adaptive and dynamic are imperative to allow use of commercial devices with reasonable risk management. (Section 4.1.2.2)

10. Management controls over application access by remote users often lack controls equivalent to those for users inside fixed facilities. (Section 4.1.2.3)
11. Research/deception networks provide valuable insight into intruder activity, as well as indicators that may be used to detect intrusion attempts. (Section 4.1.1.1.4)
12. Private sector surveys, briefings to the NSTAC, and news reports alike consistently suggest that system security managers should assume that their networks have been or will be breached. (Section 4.1.1.2)
13. Separating public facing networks containing non-critical data and functions from internal networks is an effective strategy to enhance enterprise security. (Section 4.1.1.1.2)
14. Cybersecurity is shifting from an ancillary and supporting function to part of the larger topic of risk management. (Section 4.1.2.2)
15. Having integrated cyber threat and business intelligence enables an organization's leaders to understand the positive and negative impacts of the new security strategies, personnel training, and organizational structures. (Section 4.1.3)

Behavior:

16. A key success factor of an effective cybersecurity program is attaining situational awareness through training and individual accountability, as well as empowering every employee as a security sentinel. (Section 4.2)
17. The creation and enactment of centralized security policy and standards creates an environment in which consistent measurements and metrics can be implemented. (Section 4.1.2)

Organization:

18. Establishment of a senior official for risk management across the entire organization is an industry best practice and a necessary next step for the creation of a unified approach to risk management. (Section 4.3.2)
19. Companies with sophisticated cybersecurity practices have elevated risk management issues and created a board of directors for risk management to raise awareness and enhance the security posture throughout the entire enterprise. (Section 4.3)
20. Industry has made a qualitative change in how they manage COOP. (Section 4.3)
21. Some malware will enter most systems, circumventing available protections. This lack of definitive trust in enterprise networks or systems is forcing enterprises to develop alternative means to manage risk by including consequences as part of risk management analysis. (Section 4.3.1)
22. Managing the consequences within the risk management framework is an effective strategy for enhancing cybersecurity. (Section 4.3.2)

23. In Government, centralized policy and standards do not exist for cybersecurity. (Section 4.3.2)

7.0 CONCLUSIONS

Building on the research findings identified in Section 6.0, and as a foundation for the recommendations that follow in Section, 8.0, the NSTAC's research has led to the following conclusions:

Technology: Establishing New Cybersecurity Strategies

- Modern network security processes are essential for unclassified strategies so that the Government can fully benefit from modern functionality, such as cloud, BYOD, and social media, while managing risks and consequences at acceptable levels.
- Access to and management of Web-based applications are increasingly important aspects of network security and are required components of any modern Federal security strategy or program.
- IdM efforts related to Federal networks are most effective when expanded to provide for federated controls over all network users, applications, and data wherever located.
- Federal network management policies that include continuous monitoring and rapidly adaptive controls over all users, policies, and network activities provide better network security.
- A data-centric approach to security, which incorporates a centralized policy with decentralized data that allows users to prioritize the most valuable and sensitive organizational assets, is an effective way to manage data.
- A defense-in-depth approach, such as a security kill chain, can result in a comprehensive and effective response to increased external threats targeting enterprise data.
- Non-critical data and functions should be evaluated for outsourcing to external vendors to reduce the attack surface.
- Large scale data analytics brings security authorities a previously-unavailable level of real-time situational awareness and activity analysis of their environments.

Behavior: Creating a Culture of Security

- Information security programs are a key success factor for the operation of an effective cybersecurity program.
- Executive involvement with clear messaging helps create a security culture.
- A centralized security authority with the ability to publish policy and standards is needed to elevate security awareness and create measurements for its employees.
- Effective information sharing requires information be shared across domains, their enterprises and market sectors, which results in key stakeholders receiving information in a timely and consistent manner.

Organization: Elevating Risk and Consequence Management

- Cybersecurity can be enhanced by managing consequences within a risk management framework. Best practices in improving Federal information security include elevating the visibility, authority, and accountability of centralized leadership for secure Government communications and coalescing risk management and consequence management governance.
- Industry leaders have shifted their organizational responsibilities and made qualitative changes in the way they are managing risk. The criteria of the skillset managing the risk must evolve to meet the nature of new technologies.
- Due to the expanding breadth of the threats, industry leaders must manage risk far beyond IT and telecommunications. Revolutionary technologies have caused a shift in industry's security strategies, causing industry to retrain staff to become security sentinels, thereby creating a culture of security and elevated risk management inside the industry enterprise.

8.0 RECOMMENDATIONS

Based on the authorities and responsibilities established by EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions,* the NSTAC presents the following multi-pronged recommendation to the President:

- Direct an appropriate organization to develop, adopt, and implement an integrated and balanced plan across the technological, behavioral, and organizational domains reflecting a unified strategy for more secure Government communications, as described below. Advancing in each of these three areas is not simply synergistic, but rather symbiotic; the central understanding is that the power of the strategy is only achieved by simultaneous, balanced, and coherent implementation of change in all three domains.

  The elements of this unified strategy and their related recommendations include:[72]

  1. Technology: Creating New Cybersecurity Strategies

     Modernize network security technology and adopt data-centric technology approaches to prioritize and protect data.

     - Implement security technologies and techniques providing for network defense-in-depth, embracing net users, devices, data and applications wherever located with strong and comprehensive policy oversight and adaptive controls. (Findings 1, 3, 5, 6)
     - Upgrade legacy network security technology with currently available next generation security technologies and associated processes, as defined herein, throughout Federally-managed networks; implementation to be prioritized based on elevated risk and consequence management processes discussed in this report. (Findings 2, 7, 8, 12)

[72] The parenthetical paragraph notation preceding the individual recommendation refers to the findings that support the recommendations as numbered in *Section 6.0,* Findings.

- Employ automated data analytics designed to achieve real-time contextual cybersecurity. (Finding 15)

2. Behavior: Expanding a Culture of Security

Instill in every member of every Federal organization his or her identity as a full, active, and accountable participant in organizational cybersecurity.

- Expand policies and standards to embrace all technologies and users accessing Federal networks. (Finding 16)
- Monitor, test, and evaluate all organizations and users for adherence to cybersecurity policy and standards on a rigorous and continuous basis. (Finding 17)
- Institutionalize the review and revision of behavioral policies and technology standards with frequency predicated on changing technology and the threat environment. (Finding 17)

3. Organization: Elevating Risk and Consequence Management

Elevate and qualitatively change IT and its security to become central to mission performance within each organization.

- Expand the scope of security processes beyond traditional IT to the full scope of risk management as defined herein. (Findings 18, 20, 21, 22)
- Across that full scope, establish a single centralized organization with responsibility, authority, and accountability across the Executive Branch. (Findings 18, 23)
- Replicate this process in every Federal organization at the agency-level. (Finding 19)
- Employ this cross-governmental organization to create a comprehensive, unified risk management strategy across the Federal Government within 12 months. (Finding 18)

APPENDIX A: PARTICIPANT LIST

SUBCOMMITTEE MEMBERS

Ms. Jamie Dos Santos, Chair

AT&T, Incorporated	Mr. T. Brooks Fitzsimmons
Akamai Technologies, Incorporated	Mr. Larry Underhill
Avaya, Incorporated	Mr. David Ahrens Mr. Greg Pelton
CenturyLink, Incorporated	Ms. Kathryn Condello
Communication Technologies, Incorporated	Mr. Milan Vlajnic
CSC	Mr. Guy Copeland
Frontier Communications Corporation	Mr. Pete Hayes Mr. Michael Saperstein
Harris Corporation	Mr. Stephen Reese
Juniper Networks, Incorporated	Mr. Robert Dix
Level 3 Communications, Incorporated	Mr. Dale Drew
Lockheed Martin Corporation	Mr. Macy Summers
Neustar, Incorporated	Ms. Terri Claffey
Palo Alto Networks, Incorporated	Mr. William Gravell
Raytheon Company	Mr. Michael Daly Mr. William Russ
Rockwell Collins, Incorporated	Mr. Ken Kato
Sprint Nextel Corporation	Mr. Kevin Frank
Ericsson, Incorporated	Ms. Louise Tucker
TE Connectivity, Ltd.	Mr. William O'Malley
Verizon Communications, Incorporated	Mr. Donald Tighe (Working Group Leader) Mr. Marcus Sachs

SUBJECT MATTER EXPERTS

AT&T, Incorporated	Ms. Rosemary Leffler
Booz Allen Hamilton, Incorporated	Mr. Perry Bryden

CenturyLink, Incorporated	Mr. Peter Brecl
Open Data Center Alliance	Mr. Marvin Wheeler

SUBCOMMITTEE MANAGEMENT

Booz Allen Hamilton, Incorporated	Ms. Ursula Arno
Department of Homeland Security	Ms. Sandy Benevides Mr. Michael Echols

APPENDIX B: ACRONYMS

ACD	Active Cyber Defense
APT	Advanced Persistent Threat
ATO	Authorization to Operate
BYOD	Bring Your Own Device
CCA	*Clinger-Cohen Act*
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CNCI	Comprehensive National Cybersecurity Initiative
COOP	Continuity of Operations
D/A	Department and Agency
DDoS	Distributed Denial-of-Service
DHS	Department of Homeland Security
DLP	Data Loss Prevention
DOD	Department of Defense
DoS	Denial-of-Service
EO	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISMA	*Federal Information Security Management Act*
FNR	Federal Network Resilience
FY	Fiscal Year
GAO	Government Accountability Office
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
IdM	Identity Management
ICE	Immigration and Customs Enforcement
IP	Internet Protocol
IPS	Intrusion Prevention System
IT	Information Technology
NAC	Network Access Control
NGN	Next Generation Network
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NS/EP	National Security and Emergency Preparedness
NSS	National Security Staff
NSTAC	National Security Telecommunications Advisory Committee
NSTIC	*National Strategy for Trusted Identities in Cyberspace*
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PKI	Public-Key Infrastructure
PPD	Presidential Policy Directive
SaaS	Software as a Service

SBC	Session Border Controllers
SED	Self-Encrypting Drives
SGC	Secure Government Communications
SLTT	State, Local, Tribal, and Territorial
SSL	Secure Socket Layer
TCG	Trusted Computing Group
TIC	Trusted Internet Connection
TPM	Trusted Platform Module
UC	Unified Communications
USC	United States Code
US-CERT	U.S. Computer Emergency Readiness Team
VoIP	Voice-over-Internet-Protocol

APPENDIX C: GLOSSARY

Advanced Persistent Threat: An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (National Institute of Standards and Technology [NIST] Glossary of Information Security Terms – NIST Interagency or Internal Report [IR] 7298 Revision 2)

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Availability: Ensuring timely and reliable access to and use of information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Blacklist: A list of people or things that are deemed unsafe or undesirable. (Newton's Telecom Dictionary)

Bring Your Own Device (BYOD): BYOD is a concept that allows employees to utilize their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices. This could include laptop/desktop computers; however, since mature solutions for securing and supporting such devices already exist, this document focuses on the emerging use case of mobile devices. (Whitehouse.gov)

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. (NIST Special Publication [SP] 800-145)

Communications: Modern network is the totality of users, devices, data and applications. (National Security Telecommunications Advisory Committee [NSTAC] Secure Government Communications [SGC] Subcommittee Definition)

Compartmentalization: A nonhierarchical grouping of sensitive information used to control access to data more finely than with hierarchical security classification alone. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Consequence Management: Consequence management is accomplished via methods used for increased resiliency such as system or asset redundancy, lowered dependence on other systems, fast recovery times, and infrastructure hardening. This approach might also require a de-coupling of infrastructures and services so that if a certain facility or function is disabled (via cyber or other means) its loss will have minimal impact on other facilities or functions that normally depend on it. (NSTAC SGC Subcommittee Definition)

Containerization: An aspect of network security, this term is most commonly used in relation to device management (especially wireless), wherein a generally-untrusted device – including those under the heading of "bring-your-own-device", or BYOD, as described herein – may have a more-secure "container" installed within it to encapsulate data and certificates, among others. (NSTAC SGC Subcommittee Definition)

Continuous Monitoring: The process implemented to maintain a current security status for one or more information systems or for the entire suite of information systems on which the operational mission of the enterprise depends. The process includes: 1) The development of a strategy to regularly evaluate selected IA controls/metrics, 2) Recording and evaluating IA relevant events and the effectiveness of the enterprise in dealing with those events, 3) Recording changes to IA controls, or changes that affect IA risks, and 4) Publishing the current security status to enable information-sharing decisions involving the enterprise. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Covert Communication Channel: An unauthorized communication path that manipulates a communications medium in an unexpected, unconventional, or unforeseen way in order to transmit information without detection by anyone other than the entities operating the covert channel. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Data Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Defense-in-Depth: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Emerging Technologies: New, evolving, or innovative technologies. (NSTAC SGC Subcommittee Definition)

Honeypot: A system (e.g., a Web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential hackers and intruders and has no authorized users other than its administrators. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Identity Management: The structured creation, capture, syntactical expression, storage, tagging, maintenance, retrieval, use and destruction of identities by means of diverse arrays of different technical, operational, and legal systems and practices. (International Telecommunications Union Identity Correspondence Group)

Information Security Architecture: An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Insider Threat: A malicious insider threat to an organization is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeds or misuses that access in a manner that negatively affects the confidentiality, integrity, or availability of the organization's information or information systems. (CERT Insider Threat Center)

Internet Protocol: Part of the TCP/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages; used in gateways to connect networks at OSI network Level 3 and above. (Newton's Telecom Dictionary)

Novel: New and not resembling something formerly known or used; original or striking especially in conception or style. (Merriam-Webster Dictionary)

Next Generation Network: Uses packets to transmit VoIP, data, and video technology. (Modified from Newton's Telecom Dictionary)

NS/EP Communications: Primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international); to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications also include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (National Security and Emergency Preparedness Communications Executive Committee definition based on Executive Order 13618)

Penetration Testing: Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Perimeter (Security): A physical or logical boundary that is defined for a system, domain, or enclave, within which a particular security policy or security architecture is applied. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Real-Time: The actual time during which something takes place <the computer may partly analyze the data in real-time (as it comes in). (Merriam-Webster Dictionary)

Revolutionary Technologies: Revolutionary technologies (e.g., smartphones, tablets, cloud computing, advanced laptops) that signified the advent of ubiquitous remote access and data mobility. (NSTAC SGC Subcommittee Definition)

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Secure Socket Layer (SSL): protocol used for protecting private information during transmission via the Internet. Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:." (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Smart Device: A smart device is an electronic device that is cordless (unless while being charged), mobile (easily transportable), always connected (via WiFi, 3G, 4G etc.) and is capable of voice and video communication, internet browsing, geolocation (for search purposes and location-based services) and that can operate to some extent autonomously. (NSTAC SGC Subcommittee Definition)

Social Engineering: A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Social Media: Forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos) (Merriam-Webster Dictionary)

Spam: The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Trusted Computing Platforms: Trusted computing platforms are based on a set of open, global industry standards and interoperable technologies. The concept of trusted computing is derived from the field of trusted systems, and typically is used to describe an environment of in which computers consistently behave in expected ways. Behaviors are defined by policy and enforced by hardware-based "roots of trust" at the edge of the network and at the endpoints. This root of trust is established by loading hardware with a unique encryption key inaccessible to the rest of the system. (Trusted Computing Group)

Virtual Private Network: A virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Whitelisting: A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or information system. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

APPENDIX D: BIBLIOGRAPHY

6 U.S.C § 143.

18 U.S.C. § 2510 et seq.

18 U.S.C. § 2701 et seq.

44 U.S.C. § 3541 et seq.

EO 13011, *Federal Information Technology*. July 6. 1996. Available: http://nodis3.gsfc.nasa.gov/displayEO.cfm?id=EO_13011_.

EO 13636, *Improving Critical Infrastructure Cybersecurity*. February 19, 2013. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

Amoroso, Edward G. "From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud." IEEE Computer and Reliability Societies. January/February 2013. (vol.11 no.1), ISSN: 1540-7993.

CDW. *2013 State of the Cloud Report.* February 11, 2013. Available*:* http://www.webobjects.cdw.com/webobjects/CDW-2013-State-Cloud-Report.pdf.

The Chief Information Officers Council (1999). Federal Enterprise Architecture Framework Version 1.1, September 1999.

The Chief Information Officers Council. *Guidelines for Secure Use of Social Media by Federal Departments and Agencies.* Available: https://cio.gov.

Cisco Systems, Inc "Email Attacks: This Time It's Personal." Table 3. June 2011. Available: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf.

Cohen, Reuven. "The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing." *Forbes*, April 16, 2013. Available: http://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing/.

Department of Defense. *Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Device and Removable Storage Media.* July 3, 2007. Available: http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf.

Department of Defense. "Encryption of Sensitive Unclassified Data at Rest on Mobile computing Devices and Removable Storage Media," July 3, 2007. Available: http://iase.disa.mil/policy-guidance/dod-dar-tpm-decree07-03-07.pdf.

Department of Homeland Security (DHS). "Written testimony of Acting Deputy Secretary Rand Beers for a Senate Committee on Appropriations hearing titled "Cybersecurity: Preparing for and responding to the enduring threat." June 12, 2013. Available: http://www.dhs.gov/news/2013/06/12/written-testimony-acting-deputy-secretary-rand-beers-senate-committee-appropriations

Department of Homeland Security. *If You See Something, Say Something Campaign.* Available: http://www.dhs.gov/if-you-see-something-say-something-campaign

Department of Homeland Security. *Secretary Napolitano Announces Expansion of "If You See Something, Say Something" Campaign to Wal-Mart Stores Across the Nation,"* Press Office, U.S. Dept. of Homeland Security, December 6, 2010.

Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22. October 21, 1986. Available: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap119.pdf

Computer Fraud and Abuse Act, 18 U.S.C. § 1030. Available: http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf

Executive Office of the President. *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*. Available: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Executive Office of the President. *National Security Presidential Directive 54/Homeland Security Presidential Directive 23: Comprehensive National Cybersecurity Initiative.* January 2008. Available: http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative.

Executive Office of the President. *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience.* February 12, 2013. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Federal Emergency Management Agency. "Interim Planning Guide for State and Local Governments", July 2002. Available: https://www.fema.gov/pdf/plan/managingemerconseq.pdf.

Federal Emergency Management Agency. "Contingency and Consequence Management Planning for Year 2000 Conversion: A Guide for State and Local Emergency Managers." Available: http://www.fema.gov/y2k/ccmp.htm

Gartner. *BYOD: the Facts and the Future.* Available: http://www.gartner.com/technology/topics/byod.jsp.

General Services Administration. *Using Social Media Guidelines.* Available: http://www.howto.gov/social-media/using-social-media-in-government.

General Services Administration. *Social Media Navigator.* Available: http://www.gsa.gov/portal/content/250037.

Government Accountability Office. *Cybersecurity: National Strategy, Roles and Responsibilities Need to Be Better Defined and More Effectively Implemented*, February 2013. Available: http://www.gao.gov/assets/660/652170.pdf.

Kayyem, Juliette. "Never Say 'Never Again: Our Foolish Obsession With Stopping the Next Attack." *Foreign Policy*, September 11, 2012.

Jackson, William. "Will Agencies Get Squeezed on Cybersecurity Technology?" *Government Computer News*, March 8, 2013. Available: http://gcn.com/blogs/cybereye/2013/03/agencies-squeezed-cybersecurity-technology.aspx.

Mandiant Corp. *M-Trends 2013: Attack the Security Gap*. March 13, 2013. Available: www.mandiant.com/mtrends2013.

Messmer, Ellen. "Identity management top security priority in Gartner survey; Data-loss prevention ranks second on the list," *Network World*, June 10, 2010. Available: http://www.networkworld.com/news/2010/061010-gartner-security-identity-management.html.

Microsoft Corp. *Microsoft Security Intelligence Report*. Volume 11. Available: http://download.microsoft.com/download/0/3/3/0331766E-3FC4-44E5-B1CA-2BDEB58211B8/Microsoft_Security_Intelligence_Report_volume_11_English.pdf.

National Institute of Standards and Technology. Federal Information Processing Standards Publication (FIPS PUB) 201-1, "Personal Identity Verification of Federal Employees and Contractors." March 2006. Available: http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

National Institute of Standards and Technology. FIPS PUB 201-2, "Personal Identity Verification of Federal Employees and Contractors-REVISED DRAFT." July 2012. Available: http://csrc.nist.gov/publications/drafts/...2/draft_nist-fips-201-2_revised.pdf.

National Institute of Standards and Technology. *FISMA Overview*. Available: http://csrc.nist.gov/groups/SMA/fisma/overview.html.

National Institute of Standards and Technology. "Risk Management Framework." *Special Publication 800-37 (Revision 1) Guide for Applying the Risk Management Framework to Federal Information Systems*. February 22, 2010. Available: http://www.nist.gov/customcf/get_pdf.cfm?pub_id=904985.

National Institute of Standards and Technology. *Special Publication 800-124 (Revision 1) Guidelines for Managing the Security of Mobile Devices in the Enterprise.* June 2013. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf.

National Institute of Standards and Technology. *Special Publication 800-164 Guidelines on Hardware Rooted Security in Mobile Devices (DRAFT)*. October 31, 2012. Available: http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

National Security Telecommunications Advisory Committee. *NSTAC Report to the President on Cloud Computing*, May 15, 2012. Available: https://www.dhs.gov/publication/2012-nstac-publications.

National Security Telecommunications Advisory Committee. *Cybersecurity Collaboration Report Strengthening Government and Private Sector Collaboration Through a Cyber Incident Detection, Prevention, Mitigation, and Response Capability*, May 21, 2009. Available: https://www.dhs.gov/publication/2009-nstac-publications-0.

Office of Management and Budget, U.S. Chief Information Officer*, 25 Point Implementation Plan To Reform Federal Information Technology Management*, December 9, 2010. Available: http://www.cio.gov/documents/25-point-implementation-plan-to-reform-federal%20it.pdf.

Office of Management and Budget. *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, February 3, 2011. Available: http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.

Office of Management and Budget. *Digital Management Strategy*. May 23, 2012. Available: http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html.

Office of Management and Budget. U.S. Chief Information Officer. *Federal Cloud Computing Strategy*, February 8, 2011. Available: https://cio.gov/wp-content/uploads/downloads/2012/09/Federal-Cloud-Computing-Strategy.pdf.

Office of Management and Budget. *Fiscal Year 2012 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*. March 2013. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fy12_fisma.pdf.

Office of Management and Budget. *Implementation of Trusted Internet Connections*. November 20, 2003. Available: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-05.pdf.

Office of Management and Budget. Memorandum M-*10-13 Guidance for Agency Use of Third-Party Websites and Applications.* June 25, 2010. Available: http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf.

P.L. 104-106. *Clinger-Cohen Act*. February 10, 1996. Available: https://www.fismacenter.com/Clinger%20Cohen.pdf.

P.L. 106-554. December 21, 2000. Available: http://www.gpo.gov/fdsys/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf.

P.L. 107-347. *The Federal Information Security Management Act of 2002.* December. 17, 2002.

P.L. 107-347. *E-Government Act of 2002. December 17, 2002.* Available*:* http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

The Privacy Act of 1974. December 31, 1974. Available: http://www.justice.gov/opcl/privstat.htm.

SafeGov. "Measuring What Matters: Reducing Risk by Rethinking How We Evaluate Cybersecurity." March 2013. Available: http://www.napawash.org/publications/measuring-what-matters-reducing-risk-by-rethinking-how-we-evaluate-cybersecurity/.

SANS Institute. "Methods and Techniques of Implementing a Security Awareness Program." July 2002. Available: http://www.sans.org/reading_room/whitepapers/awareness/methods-techniques-implementing-security-awareness-program_417.

Trusted Computing Group. *Trusted Computing: An Effective Approach to Cybersecurity Defense."* April 2013. Available: http://csrc.nist.gov/cyberframework/rfi_comments/040413_tcg.pdf.

United States Constitution. Available: http://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf.

Veracode. *Data Loss Prevention Guide.* Available: http://www.veracode.com.

Verizon Communications, Inc. *Data Breach Investigations Report 2013*. April, 2013. Available: http://verizonenterprise.com/DBIR/2013.

Virtustream. *Security in the Cloud: Is it Pie in the Sky?* Available: http://www.virtustream.com/cloud_platform/enterprise_class_iaas.

Willis, David A. "Bring Your Own Device: The Facts and the Future." *Gartner*. April 11, 2013.

Briefings

Akers, Gregory. Cisco Systems, Inc. "Cisco Pervasive Security Overview." March 27, 2013.

Amoroso, Ed. AT&T, Inc. "From the Enterprise Perimeter to a Mobility-Enabled Secure Cloud."

February 27, 2013.

Beernink, Kurt, Doug Gardner and William Keely. Defense Information Systems Agency, Department of Defense. "NSTAC Briefing." February 20, 2013.

Carey, Robert. Department of Defense. "Moving to Mobile." March 20, 2013.

Collie, Byron. Goldman Sachs. "NSTAC Briefing." March 19, 2013.

Crane, Earl. National Security Staff. "NSTAC Briefing." January 16, 2013.

Croom, Lieutenant General Charles (Retired). Lockheed Martin Corporation. "Intelligence Driven Defense," January 23, 2013.

Dodson, Donna. National Institute of Standards and Technology. "NSTAC Briefing". March 13, 2013.

Finan, Chris and Dan Roelker. Defense Advanced Research Project Agency. "NSTAC Briefing". February 20, 2013.

Gagnon, Gary. MITRE. "Operationalizing Threat Intelligence into Cyber Defense." March 20, 2013.

Geddis, Shawn. Apple. "BYOD: Where can it take us?" February 6, 2013.

Goldthorp, Jeffery. Federal Communications Commission. "NSTAC Briefing". March 13, 2013.

Goode, Brendan. Network Security Deployment Division, Department of Homeland Security. *NSTAC Briefing*. January 16, 2013.

Groose, Eric, David Mihalchik and Michele Weslander-Quaid. Google. "NSTAC Briefing". February 13, 2013.

Hall, Dean and Patrick Reidy. Federal Bureau of Investigation. "NSTAC Briefing". April 24, 2013.

Kizzee, Carlos. Department of Homeland Security. "NSTAC Briefing." March 26, 2013.

Klarich, Lee. Palo Alto Networks. "The Need for Next-Generation Security," February 6, 2013.

Koretz, David. Mykonos Software. "The Smartest Way to Protect Websites and Web Apps from Attacks," January 23, 2013.

Kuper, Peter. In-Q-Tel. "NSTAC Briefing". March 15, 2013.

Lawhorn, Brian. Kroger. "NSTAC Briefing". March 27, 2013.

Ledgett, Rick. National Security Agency. “NSTAC Briefing.” February 20, 2013.

Maestri, Phil. Department of Education. “NSTAC Briefing.” May 8, 2013.

McGovern, Mark. MobileSystems7. “Strategic Security Issues and Opportunities.” March 12, 2013.

McKnight, Tim. Fidelity Investments. “NSTAC Briefing”. February 6, 2013.

McMahan, Doug. Verizon. “BYOD Into the Workplace.” March 13, 2013.

Mosley, Sara and Marilyn Rose. Federal Network Resilience Division, DHS. “Federal Cybersecurity Reference Architectures.” January 16, 2013.

Nigriny, Jeff. Certi Path, the Aerospace/Defense PKI Bridge. “The Biggest Cyber Threat: Interoperability,” March 20, 2013.

Portale, Joseph. Lockheed Martin Corporation. “Enterprise Mobility.” January 23, 2013.

Sager, Tony. SANS Institute. “Critical Security Controls.” January 30, 2013.

Shepherd, Lewis. Microsoft. “The Evolution of Security Thought and Practice Within a Large Bureaucracy: How Microsoft Secures and Protects Critical Communications and Data.” February 13, 2013.

Streufert, John. Federal Network Resilience Division, DHS. “Continuous Diagnostics and Mitigation Program.” January 16, 2013.

Taran, Gabriel. Office of General Counsel, DHS. “NSTAC Briefing.” March 26, 2013.

Weber, Dean. CSC. “NSTAC Briefing: Advancing the Cloud.” February 13, 2013.

APPENDIX E: CYBERSECURITY LAWS

There are several Federal cybersecurity laws that are relevant to secure Government communications and may require Federal Government review.

The *Federal Information Security Management Act*

The *Federal Information Security Management Act* (FISMA) outlines a comprehensive risk-based framework to help ensure the effectiveness of information security controls over information resources that support Federal operations and assets. The act requires each agency to develop, document, and implement an information security program. Under FISMA, the Office of Management and Budget (OMB) has the following responsibilities:[73]

- Developing and overseeing the implementation of policies, principles, standards, and building on information security in Federal agencies (except with regard to national security systems)[74]; and
- Annually reviewing and approving agency information security programs.

Also under FISMA, the National Institute for Standards and Technology (NIST) is responsible for developing security standards and guidelines for agencies that include standards for categorizing information and information systems according to ranges of risk levels, minimum security requirements for information and information systems in risk categories, guidelines for detection and handling of information security incidents, and guidelines for identifying an information system as a national security system.[75,76]

The *Clinger-Cohen Act*

The *Clinger-Cohen Act of 1996* (CCA) replaced the *Information Technology Management Reform Act of 1996*. The CCA was developed to improve the Federal Government's acquisition laws and information technology management.[77] The CCA:

- Requires each agency to name a chief information officer (CIO) who is responsible for "developing, maintaining, and facilitating the implementation of a sound and integrated

[73] OMB has since assigned its oversight responsibilities under FISMA to the Department of Homeland Security (DHS) in its memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security*.

[74] As defined in FISMA, the term " national security system" means any information system used by or on behalf of a Federal agency that (1) involves intelligence activities, national security-related cryptologic activities, command and control of military forces, or equipment that is an integral part of a weapon or weapons system, or is critical to the direct fulfillment of military or intelligence missions (excluding systems used for routine administrative and business applications); or (2) is protected at all times by procedures established for handling classified national security information. See 44 U.S.C. § 3542(b)(2).

[75] NIST standards and guidelines, like OMB policies, do not apply to national security systems.

[76] Under the *Cyber Security Research and Development Act* NIST is responsible for developing a checklist of settings and option selections to minimize security risks associated with computer hardware and software widely used within the Federal Government.

[77] P.L. 104-106. The *Clinger-Cohen Act of 1996*. February 10, 1996. Available: https://www.fismacenter.com/Clinger%20Cohen.pdf.

information technology architecture." The CIO is tasked with advising the agency director and senior staff on all IT issues. It elevated overall responsibility to the OMB Director.

- Directs the development and maintenance of Information Technology Architectures by Federal agencies to maximize the benefits of the Government's information technology (IT).[78]

CIOs also formed the CIO Council, which was established by Executive Order 13011, *Federal Information Technology*, and codified into law by the *E-Government Act of 2002*.[79,80] The council is responsible for developing recommendations for Government information technology management policies, procedures, and standards; identifying opportunities to share information resources; and assessing and addressing the needs of the Federal Government's IT workforce.[81]

Other Statues that Impact the Federal Cybersecurity Posture

- The *Privacy Act of 1974* requires agencies to file a system of records notice for systems that include personally identifiable information.[82]
- The *E-Government Act of 2002* requires Federal agencies to complete a privacy index of applications that use information technology.[83]
- The *Computer Fraud and Abuse Act* is a criminal statute that addresses computer fraud. This law criminalizes unauthorized access, exceeding the scope of one's authorized access to the system, and sending commands to an information system with the intent to cause harm without authorization.[84] Federal agencies conduct penetration tests to ensure compliance and provide evidence for granting an authorization to operate (ATO) systems. Agencies must have an ATO from their CIO or authorized representative.
- The Fourth Amendment of the United States Constitution addresses unreasonable search and seizure of information.[85]
- The *Electronic Communications Privacy Act* addresses electronic communications, and includes:[86]

[78] The Chief Information Officers Council (1999). Federal Enterprise Architecture Framework Version 1.1, September 1999.

[79] EO 13011, *Federal Information Technology*. July 6. 1996. Available: http://nodis3.gsfc.nasa.gov/displayEO.cfm?id=EO_13011_.

[80] P.L. 107-347. *E-Government Act of 2002. December 17, 2002.* Available*:* http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

[81] The Chief Information Officers Council. Available: https://cio.gov.

[82] *The Privacy Act of 1974*. December 31, 1974. Available: http://www.justice.gov/opcl/privstat.htm.

[83] P.L. 107-347. *E-Government Act of 2002.* December 17, 2002. Available*:* http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/html/PLAW-107publ347.htm.

[84] *Computer Fraud and Abuse Act*, 18 U.S.C. § 1030. Available: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap47.htm.

[85] United States Constitution. Available: http://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf.

[86] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22. October 21, 1986. Available: http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap119.pdf.

- The *Stored Communications Act,* which, among other things, prescribes under what circumstances email providers (e.g., Yahoo and Gmail) can share emails with law enforcement;[87]
- The *Wiretap Act* prohibits the interception, use, or disclosure of communications. There are national security exceptions to this act; companies can comply with the Act's requirements by asking users to sign a form consenting to having their communications monitored.[88]

- The *Data Quality Act (DQA)* passed in Section 515 of the *Consolidated Appropriations Act 2001* (Public Law 106-554). [89,90] The DQA directs OMB to issue Government-wide guidelines that "provide policy and procedural guidance to Federal agencies for ensuring and maximizing the quality, objectivity, utility, and integrity of information (including statistical information) disseminated by Federal agencies."

<u>Other Laws and Directives Affecting Cyber Security</u>

Various laws and directives have also given Federal agencies responsibilities for the protection of critical infrastructures, which are largely owned by private sector organizations. The *Homeland Security Act of 2002* created the Department of Homeland Security (DHS). DHS is responsible for (1) developing a comprehensive national plan for securing the critical infrastructures of the United States; (2) recommending measures to protect those critical infrastructures in coordination with other groups; (3) disseminating, as appropriate, information to assist in the deterrence, prevention, and preemption of, or response to, terrorist attacks and other disasters; and (4) providing to owners and operators of critical information systems warnings about cybersecurity threats and vulnerabilities to those systems.[91]

DHS also provides operational support to Federal agencies' IT systems through the United States Computer Emergency Readiness Team.

Presidential Policy Directive (PPD) 21, *Critical Infrastructure Security and Resilience,* was issued in February 2013, and supersedes Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection,* which was issued in December 2003. PPD-21 establishes policy on critical infrastructure security and resilience as a shared responsibility among the Federal, State, local, tribal, and territorial entities, and public and private owners and operators of critical infrastructure. PPD-21 provides that the Federal Government has a responsibility to strengthen the security and resilience of its own critical infrastructure, for the continuity of national essential functions, and to organize itself to partner effectively with and add value to the security and resilience efforts of critical infrastructure owners and operators. PPD-21 directs the Secretary of Homeland Security to provide strategic

[87] 18 U.S.C. § 2701 et seq.
[88] 18 U.S.C. § 2510 et seq.
[89] No name was given in the actual legislation; the Government Accountability Office refers to it as the Information Quality Act, while others refer to it as the Data Quality Act.
[90] Public Law 106-554. December 21, 2000. Available: http://www.gpo.gov/fdsys/pkg/PLAW-106publ554/pdf/PLAW-106publ554.pdf.
[91] See 6 U.S.C § 143.

guidance, promote a national unity of effort, and coordinate the overall Federal effort to promote the security and resilience of the Nation's critical infrastructure.[92]

[92] Executive Office of the President. *Presidential Policy Directive 21, Critical Infrastructure Security and Resilience*. February 12, 2013. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

APPENDIX F: TESTIMONY ON DHS FUNDED PROGRAMS

The Department of Homeland Security's (DHS) Fiscal Year (FY) 2014 budget includes funding for several cybersecurity initiatives. In his June 12, 2013, testimony for a Senate Committee on Appropriations, Acting Deputy Secretary Rand Beers outlined the following initiatives:[93]

- **Federal Network Security:** $200 million is included for Federal Network Security, which manages activities designed to enable Federal agencies to secure their IT networks. The Budget provides funding to further reduce risk in the Federal cyber domain by enabling continuous monitoring and diagnostics of networks in support of mitigation activities designed to strengthen the operational security posture of Federal civilian networks. DHS will directly support Federal civilian departments and agencies in developing capabilities to improve their cybersecurity posture and to better thwart advanced, persistent cyber threats that are emerging in a dynamic threat environment.

- **National Cybersecurity & Protection System (NCPS)**: $406 million is included for Network Security Deployment, which manages NCPS, operationally known as EINSTEIN. NCPS is an integrated intrusion detection, analytics, information-sharing, and intrusion-prevention system that supports DHS responsibilities to defend Federal civilian networks.

- **United States Computer Emergency Readiness Team (US-CERT)**: $102 million is included for operations of US-CERT, which leads and coordinates efforts to improve the Nation's cybersecurity posture, promotes cyber information sharing, and manages cyber risks to the Nation. US-CERT encompasses the activities that provide immediate customer support and incident response, including 24-hour support in the National Cybersecurity and Communications Integration Center. As more Federal network traffic is covered by NCPS, additional US-CERT analysts are required to ensure cyber threats are detected and the Federal response is effective.

- **State, Local, Tribal, and Territorial (SLTT) Engagement**: In FY 2014, DHS will expand its support to the Multi-State Information Sharing and Analysis Center (MS-ISAC) to assist in providing coverage for all 50 states and 6 U.S. territories in its managed security services program. MS-ISAC is a central entity through which SLTT governments can strengthen their security posture through network defense services and receive early warnings of cyber threats. In addition, the MS-ISAC shares cybersecurity incident information, trends, and other analysis for security planning.

- **Cybersecurity Research and Development:** The FY 2014 Budget includes $70 million for the DHS Science and Technology Directorate's research and development focused on strengthening the Nation's cybersecurity capabilities.

[93] The indicatives listed below are encompassed in the Written testimony of Acting Deputy Secretary Rand Beers for a Senate Committee on appropriations hearing titled "Cybersecurity: Preparing for and responding to the enduring threat." Available: http://www.dhs.gov/news/2013/06/12/written-testimony-acting-deputy-secretary-rand-beers-senate-committee-appropriations.

- **Cyber Investigations:** The FY 2014 budget continues to support Immigration and Customs Enforcement (ICE) and the Secret Service to strategically investigate domestic and international criminal activities, including computer fraud, network intrusions, financial crimes, access device fraud, bank fraud, identity crimes and telecommunications fraud, benefits fraud, arms and strategic technology, money laundering, counterfeit pharmaceuticals, child pornography, and human trafficking occurring on or through the Internet. The Budget continues to enable these DHS law enforcement agencies to provide computer forensics support and training for law enforcement partners to enable them to effectively investigate cyber crime and conduct other highly-technical investigations. ICE projects an FY 2014 expenditure of $13.8 million for the Cyber Crimes Center supporting investigations to identify, disrupt, and dismantle domestic and transnational criminal organizations engaged in crimes facilitated by use of computers and cyberspace. In addition, ICE expects to spend $96.5 million on investigations of cyber crime/child exploitation. Other investigations of illicit trade, travel and finance all make use of cyber investigative techniques including computer forensic analysis. The Secret Service's Electronic Crimes Task Force will also continue to focus on the prevention of cyber attacks against U.S. financial payment systems and critical infrastructure through aggressive investigation and information sharing.

- **Cyber Protection:** The FY 2014 budget includes $13.5 million to enhance the Secret Service's ability to secure protective venues, National Special Security Events and associated critical infrastructure/key resources from cyber attacks.

APPENDIX G: APPROACHING THE PROBLEM

At the highest level, the NSTAC approached secure Government communications in classic ways that have been modernized and refined for the specific nature of today's risk and opportunities. This approach requires systems architects and managers to address several key questions, listed below.

Prevention: How can the introduction of malware be most reliably prevented?

Firewalls remain the epicenter of security technology; however, to be effective, firewalls must be updated and evolve into a more application-aware and adaptive set of layered functions. Firewalls have the ability to identify and control applications, users, and content, regardless of the port, protocol, or Internet protocol address. Speed and agility are essential for this effort; these must be linked and keyed to continuous threat and network analytics and forensics.

A recent tendency to introduce stand-alone and single-purpose security technologies (e.g. software that only detects spyware) contributes to the overall issue. These technologies are signature-based, missing any changes in the malware's footprint. Additionally, single-purpose security technologies are generally not the same as devices that can remove malware once discovered on a system.

Detection: How can threats be most reliably detected and understood?

The threat landscape has rapidly evolved, and is both dynamic and opportunistic; no matter how strong network administrators attempt to block known ports, the threat adapts to find openings in unexpected places, exploiting vulnerabilities throughout the enterprise. Attackers have increasingly leveraged applications, commonly called "apps," to introduce malware. The prevalence of application-introduced malware was relatively insignificant when applications were pre-loaded onto devices at initial delivery; however, today's consumerization of information technology has enabled application developers and vendors to aggressively market attractive features to users and make them available at little or no cost. This process circumvents any configuration control and security strategies that user organizations implement. Today, uncontrolled access to downloadable applications is the single greatest threat to end-user devices and networks as a vehicle for malware introduction. It is important to note that because of the proliferation of desktop and mobile-device operating systems, all users can be implicated and become targets.

Since 2007, applications have bypassed detection and control by traditional security infrastructure, including firewalls, intrusion prevention systems, proxies, and universal resource locator filters. Malicious actors have leveraged applications to gain undetected network access; any attempt to detect this new type of threat must start by having full visibility into all applications. These issues are further compounded by the significant growth of host operating systems.

Containment: How can continuous analysis of the threat/response environment be used to tune security management to prevent malware or attackers from roaming through interconnected networks?

Real-time and forensic analysis permits continuous monitoring of applications' use and performance within a system to contain and limit the impact of malware, external attacks, or insider threats, enhancing situational awareness as well as security. Analyzing the data provided by continuous monitoring will create actionable results. Using virtual containers (or containerization) allows data protections to be implemented closer to critical data than traditional perimeter protections, and can limit the ability of a breach to progress through interconnected networks and systems. By limiting application usage through containers, controlling access based on user identity, and blocking known threats, near-real-time application and content analysis across networks becomes easier.

It is likely that some malware will successfully enter systems, circumventing even the most advanced firewalls or standalone security devices. Continuous analysis and containment are needed to permit defenses to be revised based on encountered threat behavior, and to discern the extent and type of malware that has escaped initial detection and entered networks and systems. These metrics are valuable for measuring how long it took an organization to detect the intrusion and how long it takes to mitigate the compromise.

Remediation: How can threats that circumvent all protections be most effectively removed, and any damage repaired?

The ability to find embedded malware is only part of the issue; it must also be completely removed with minimal disruption of the systems and processes where it resides. It is increasingly important for there to be a connection between network security and host security, which often does not exist. This link allows direct transference from threat detection to remediation. In order to enable situational awareness and avoid duplicative efforts across an enterprise, it is necessary to have a centralized authority for an organization to share incident and mitigation techniques with other organizations.