Information Technology Sector-Specific Plan

An Annex to the NIPP 2013

2016

Homeland Security

Table of Contents

Letter from the Council Chairs

The Department of Homeland Security designed this Information Technology Sector-Specific Plan (ITSSP) to guide the Sector's voluntary, collaborative efforts to improve security and resilience over the next four years. The ITSSP describes how the Information Technology Sector manages risks and contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21. As an annex to the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), this ITSSP tailors the strategic guidance provided in the NIPP 2013 to the unique operating conditions and risk landscape of the Information Technology Sector. The Sector strategy closely aligns with the NIPP 2013 national strategy, the 2014 Joint National Priorities, and Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*.

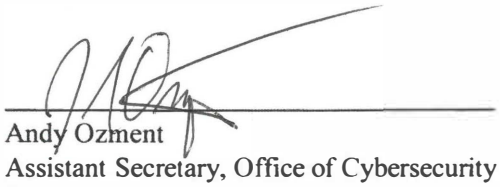
This 2016 release of the ITSSP serves as an update to the original plan issued in 2010. This ITSSP represents a collaborative effort among the private sector; State, local, tribal, and territorial (SLTT) governments; nongovernmental organizations; and Federal departments and agencies to identify and work toward shared goals and priorities to reduce critical infrastructure risk.

The Information Technology Sector Coordinating Council (SCC) and Government Coordinating Council (GCC) jointly developed the Information Technology Sector goals, objectives, and activities in this ITSSP, which collectively reflect the overall strategic direction for the Sector as a whole.

This ITSSP also reflects the maturation of the Information Technology Sector partnership and the progress made to address the evolving risk, operating, and policy environments. Since 2010, Information Technology Sector partners in the public and private sectors have taken significant steps to reduce Sector risk, improve coordination, and strengthen security and resilience capabilities.

In the same shared purpose that guided these actions and their support for the framework, concepts, and processes outlined in the NIPP 2013 and EO 13636, Information Technology Sector partners look forward to continuing their efforts to enhance the security and resilience of our Nation's critical infrastructure assets.

John Miller
Chair
Information Technology, Sector Coordinating Council



Andy Ozment
Assistant Secretary, Office of Cybersecurity and Communications
U.S. Department of Homeland Security

Caitlin Durkovich
Assistant Secretary, Office of Infrastructure Protection
U.S. Department of Homeland Security

Executive Summary

The Information Technology (IT) Sector produces and provides high-assurance IT products and services for governments, critical infrastructure sectors, commercial businesses, and private citizens around the globe. Government and industry partnership is critical to creating a continuous risk reduction system across a Sector as large and diverse as the IT Sector. To meet these challenges, effective collaboration among public and private sector partners is imperative to ensure the protection and resilience of IT Sector functions upon which the Sector and Nation depend. With critical infrastructure protection being the primary concern, the IT Sector's vision is "to achieve a sustained reduction in the impact of incidents on the Sector's critical functions."

Many critical infrastructure Sectors are primarily composed of finite and easily identifiable physical assets. Unlike some other Sectors, the IT Sector is a functions-based Sector that comprises not only physical assets, but also virtual systems and networks that enable key capabilities and services in both the public and private sectors. Six critical functions support the Sector's ability to produce and provide high-assurance IT products and services for various Sectors. These functions are required to maintain or reconstitute networks (e.g., the Internet, local networks, and wide area networks) and their associated services. The IT Sector's six critical functions are:

1. Provide IT products and services;
2. Provide incident management capabilities;
3. Provide domain name resolution services;
4. Provide identity management and associated trust support services;
5. Provide Internet-based content, information, and communications services; and
6. Provide Internet routing, access, and connection services.

These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—that provide IT hardware, software, systems, and services. IT services include development, integration, operations, communications, and security.

The private sector, which constitutes the owners and operators of the majority of Information Technology infrastructure, is the primary entity responsible for protecting Sector infrastructure and assets. Working with the Federal Government, The Information Technology Sector Coordinating Council (IT SCC) and Government Coordinating Council (IT GCC) coordinated to develop an update to the 2010 Information Technology Sector-Specific Plan (ITSSP) in accordance with the *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013). In this 2016 ITSSP, the IT SCC and IT GCC have identified priorities to guide the Sector's security and resilience efforts over the next four years. The priorities include activities surrounding risk management, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, situational awareness, information sharing, and partnership and engagement. These efforts are conducted with the broader context of the global nature of IT Sector interests and activities.

1. Introduction

The Information Technology (IT) Sector provides products and services that support the efficient operation of today's global information-based society. These products and services are integral to the operations and services provided by other critical infrastructure Sectors. While IT Sector operations, products, services, and functions enhance efficiency and effectiveness and increase the resilience of the Sector, they face numerous multifaceted global threats from natural and manmade events on a daily basis. Many of these events occur frequently but do not have significant consequences because of individual entities' existing security and response capabilities.

The purpose of the IT Sector-Specific Plan (ITSSP) is to guide and align the Sector's efforts to secure and strengthen the resilience of critical infrastructure and describe how the IT Sector contributes to national critical infrastructure security and resilience, as set forth in Presidential Policy Directive 21 (PPD-21). This SSP tailors the strategic guidance provided in the 2013 National Infrastructure Protection Plan (NIPP 2013) to the unique operating conditions and risk landscape of the IT Sector.

This SSP represents a collaborative effort among State, local, tribal, and territorial (SLTT) governments; non-governmental organizations; Federal departments and agencies; and private industry to establish common goals to reduce critical infrastructure risk. It also reflects the maturation of the IT Sector partnership and the progress made by the Sector since the 2010 ITSSP to address the evolving risk, operating, and policy environments.

2. Sector Overview

2.1 Sector Profile

The IT Sector provides products and services that support the efficient operation of today's global information-based society and are integral to the operations and services provided by other critical infrastructure Sectors. The IT Sector is comprised of small and medium businesses, as well as large multinational companies. Unlike many critical infrastructure Sectors composed of finite and easily identifiable physical assets, the IT Sector is a functions-based Sector that comprises not only physical assets but also virtual systems and networks that enable key capabilities and services in both the public and private sectors.

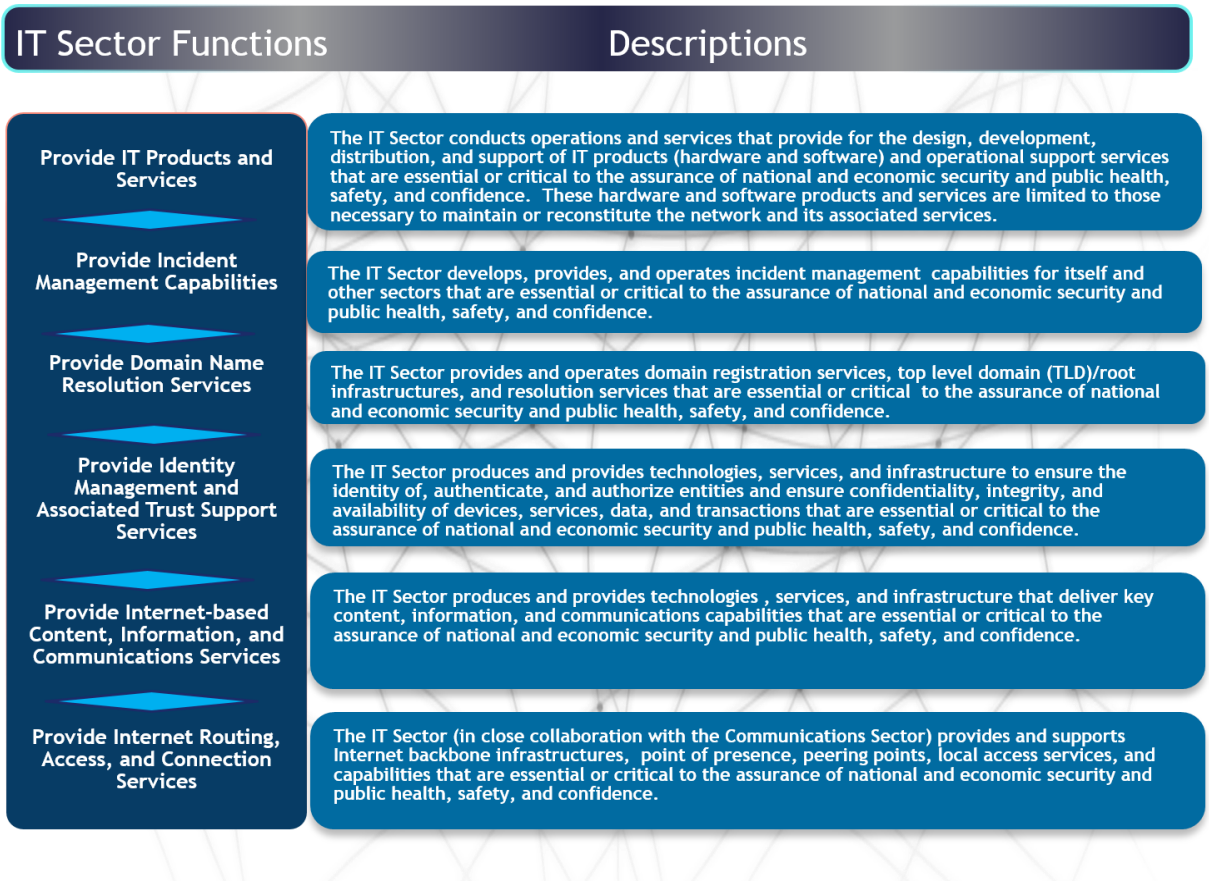
The IT Sector functions encompass the full set of processes involved in creating IT products and services, including Research and Development (R&D), manufacturing, distribution, upgrades, and maintenance. They also support the Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. Assurance is essential to achieving the Sector's vision and is therefore a fundamental aspect of all critical functions. The functions are not limited by geographic or political boundaries, further defining its virtual and distributed nature. This distribution highlights the increasing need for international collaboration and coordination for risk assessment activities, effective security practices, and protective program design and implementation. Additionally, the critical functions may be developed and maintained by small, medium, or large companies with varied resources and capabilities highlighting the need for risk management strategies and protective programs that map and scale to a wide range of needs.

2.1.1 IT Sector Critical Functions

Six critical functions support the Sector's ability to provide high assurance IT products and services for various Sectors. These functions (Figure 2-1) are required to maintain or reconstitute networks (e.g., the Internet, local networks, and wide area networks) and their associated services. The functions reflect the IT Sector Coordinating Council's (SCC) and Government Coordinating Council's (GCC) consensus on critical functions derived from the 2009 IT Sector Baseline Risk Assessment (ITSRA) that are vital to the Nation's economic security and public health, safety, and confidence. These functions are distributed across a broad network of infrastructure, managed proactively, and therefore, can withstand and rapidly recover from most threats.

These critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—who provide IT hardware, software, systems, and services. IT services include development, integration, operations, communications, testing, and security.

Figure 2-1: IT Sector Functions



2.2 IT Sector Evolution since the 2010 SSP

Over the past five years, many changes have occurred across the information and communications technology ecosystem. These changes have influenced, and will continue to influence, how the IT Sector looks at and responds to risks to its critical infrastructure. Among the noteworthy trends in technology are:

- Increasing adoption of cloud computing by enterprises and consumers;
- Massive growth in mobile computing and mobile applications for smartphones and tablets;
- Expanding awareness and deployment of the Internet of Things (IoT) and the trend in smart sensors/smart devices controlling physical systems (cyber physical domain);
- Extensive organizational acceptance of Bring Your Own Device (BYOD) in the corporate environment and the collapse of the perimeter as a defense;
- Increasing reliance on advanced analytics/Big Data;
- Ever-increasing IT operational complexity, and;
- Unrelenting, global rise in the demand for IT services and products.[1]

As a result of these continuing trends, cyberspace—the globally interconnected digital information and communications infrastructure—has become a constant in society, rapidly transforming individual and

[1] Other trends include the widespread use of server virtualization in data centers, massive growth in social networking, continuing emergence of software defined networking, and the continuing arrival of wearable technology and 3-D printing.

organizational life. Critical infrastructure Sectors, in the U.S. and overseas, depend heavily on interconnected IT systems and architectures to support the Nation's economy, public safety, and national security and resilience. One item alone, the IoT, as noted in a recent National Security Telecommunications Advisory Committee (NSTAC) report, will "increase in both speed and scope, and […] will impact virtually all Sectors of our society."[2]

Accompanying the constant trends in the IT Sector, however, have been the constant and ever-increasing threats to the IT Sector. Those threats are complex and varied, presenting severe economic impact and national security concerns. The IT Sector faces cyber and physical dangers at the hands of criminals, hackers, terrorists, and nation-states, all of whom have demonstrated multiple capabilities and intentions to attack critical IT Sector functions. Manmade threats have rapidly evolved from physical sabotage and simple automated worms and viruses, to complex social engineering attacks that exploit known and unknown vulnerabilities in IT products and services. Traditional security approaches need to be constantly expanded to address next-generation malware.

Recognizing the importance of cybersecurity, the U.S. Federal Government has taken multiple steps to address both old and new threats faced by the Nation's IT Sector and other critical infrastructure Sectors. On February 12, 2013, President Obama signed Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (PPD-21), which described a national effort to secure and strengthen the resilience of the Nation's critical infrastructure. The President simultaneously issued Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity in February 2013, which called on the Federal Government to work closely with critical infrastructure owners and operators to improve information sharing and collaboratively develop and implement risk-based approaches to cybersecurity. The coordinated release of these two policies was a catalyst to a series of measures enacted to improve approaches to critical infrastructure risk management, policy, and operating environments.

These policy measures led to an update of the NIPP 2013. The NIPP established a risk management plan based on voluntary private-public collaboration that would improve security and resilience in critical infrastructure Sectors before, during, and after incident management situations. The NIPP 2013 includes 12 Calls to Action (CtA), which guide the collaborative efforts of the critical infrastructure community to advance security and resilience under three broad activity categories: building upon partnership efforts, innovating in managing risk, and focusing on outcomes.

Along with the other critical infrastructure Sectors, the IT Sector is impacted by the changing risk and policy landscape since 2010. Given the dependence of the other infrastructure Sectors on the critical functions provided by the IT Sector, the IT Sector is particularly motivated to work collaboratively to implement improved cybersecurity and cyber resilience practices.

2.3 Sector Risks

The IT Sector has identified its five greatest risks of concern facing the six critical functions of the Sector in the 2009 ITSRA. These risks of concern are validated and updated during subsequent risk assessments conducted by the Sector on a regular basis. The IT Sector has focused its risk management activities on these areas. These risks and associated mitigations are depicted in Table 2-1.

[2] National Security Telecommunications Advisory Committee (NSTAC) Report to the President on the Internet of Things, 19 November 2014. https://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf. Accessed November 18, 2015.

Table 2-1: IT Sector Functions, Risks, and Mitigations

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Produce and Provide IT Products and Services	• Production or distribution of untrustworthy critical product/service through a successful manmade deliberate attack on a supply chain vulnerability *(Consequence: High; Likelihood: Low)*	• Supply chain resilience though redundancy and process controls -*Existing Mitigation* • Sourcing strategies (i.e., careful monitoring of the availability and quality of critical raw materials) -*Existing Mitigation* • Product recall informed by situational awareness and timely response to compromised production -*Existing Mitigation*
Provide Domain Name Resolution Services	• Breakdown of a single interoperable Internet through a manmade attack, and resulting failure of governance policy *(Consequence: High; Likelihood: Medium)* • Large scale manmade Denial-of-Service attack on the Domain Name System (DNS) infrastructure *(Consequence: High; Likelihood: Low)*	• Processes that enhance quality assurance and ensure continuous monitoring of DNS infrastructure -*Existing Mitigation* • Provisioning and the use of Anycast -*Existing Mitigation* • Infrastructure diversity and protection enhanced redundancy and resiliency -*Mitigation Being Enhanced*
Provide Internet-based Content, Information, and Communications Services	• Manmade unintentional incident caused in Internet content services result in a significant loss of e-Commerce capabilities *(Consequence: High; Likelihood: Negligible)*	• Policy and access controls -*Existing Mitigation* • Security training for users and small businesses -*Mitigation Being Enhanced* • Enhance rerouting capabilities of the Communications and IT Sectors -*Potential Future Mitigation*
Provide Internet Routing, Access, and Connection Services	• Partial or complete loss of routing capabilities through a deliberate manmade attack on the Internet routing infrastructure *(Consequence: High; Likelihood: Low)*	• Enhanced routers (i.e., increased speed, reliability, and capacity of routers and router software) -*Existing Mitigation* • Responsiveness to increasing Internet traffic -*Mitigation Being Enhanced* • Increase physical security of Network Access Points and Internet Exchange Points -*Mitigation Being Enhanced* • Improved incident response including contingency planning, training, and investment to enable skilled technicians to monitor networks to identify and respond to anomalies, outage, or incident -*Mitigation Being Enhanced*
Provide Incident Management Capabilities	• Impact to detection capabilities due to lack of data availability resulting from a natural threat *(Consequence: High; Likelihood: Medium)*	• National-level incident response and coordination capabilities -*Existing Mitigation* • Infrastructure and workforce diversity -*Existing Mitigation* • Information sharing enhancements creating common situational awareness -*Existing Mitigation*

2.4 Critical Infrastructure Partners

The NIPP 2013 describes a sector partnership model that encourages the public and private sectors to collaborate on their respective infrastructure protection activities. This collaboration is accomplished through SCCs, comprised of industry and private-sector partners, and GCCs, comprised of Federal, State, local, tribal, and territorial government entities.

The IT SCC and GCC are the primary bodies for communicating their respective perspectives and developing collaborative policies, strategies, and security efforts to advance critical infrastructure protection.

2.4.1 Sector Membership

Sector-Specific Agency

PPD-21 assigns the Department of Homeland Security (DHS)the task of Sector-Specific Agency (SSA) for the IT Sector. Within DHS, the National Protection and Programs Directorate (NPPD) Office of Cybersecurity and Communications (CS&C) provides leadership for the IT Sector as the IT Sector SSA.

IT Government Coordinating Council

The IT GCC, with representation from Federal and SLTT governments, is the public sector component of the IT Sector public-private partnership model. The objective of the GCC is to effectively coordinate within the IT Sector and provide resilience strategies and activities, policy, and communication across government and between government and the Sector to support the Nation's IT infrastructure and homeland security mission.

The IT GCC comprises Federal, State, and local governments as providers of IT services that meet the needs of citizens, businesses, and employees. The IT GCC meets at least semi-annualy to discuss and provide the most current information on relevant security and resilience programs, activities, and issues across the partnership. A current list of IT GCC members, including the Departments of Commerce, Defense, Energy, and Treasury, as well as various DHS components and agencies, can be found in Appendix A.

IT Sector Coordinating Council

The IT SCC, which is a self-organized, self-run, and self-governed private sector council consisting of critical infrastructure owners and operators and their representatives, provides a forum for members of the private sector to discuss infrastructure protection issues among themselves or to communicate with the government through the GCC. The IT SCC enables IT system owners and operators of all sizes to coordinate on a wide range of sector-specific strategies, policies, activities, and issues related to the security and resilience of the Sector. IT Sector owners and operators are vital contributors to IT SCC implementation-level initiatives. A current list of the IT SCC members can be found in Appendix A.

The IT SCC is comprised of private sector entities representing:

- Communications companies that characterize themselves as having an IT role
- Domain Name System (DNS) root and Generic Top-Level Domain (gTLD) operators
- Edge and core service providers
- Internet backbone providers
- Internet portal and e-mail providers
- Internet service providers (ISP)
- IT security associations
- IT system integrators
- Networking hardware companies
- Network Security Information Exchange (NSIE)
- Software companies

- Security services vendors

IT Sector Partnership Model

Collaboration among public and private sector partners is critical to ensure the security and resilience of IT Sector functions upon which the Sector and Nation depend. One of the IT Sector's priorities is to strengthen our Critical Infrastructure partnership both domestically and internationally to enhance information sharing, increase situational awareness, improve incident response capabilities and overall incident management, and coordinate strategic policy issues.

Specific Outcomes that the IT Sector is working to achieve include:

- Externally institutionalizing and innovating effective structures and processes between the IT SCC, IT GCC, United States Government, and other critical infrastructure partnerships to enhance security and resilience both domestically and internationally;
- Internally institutionalizing and innovating effective structures and processes within the IT Sector Coordinating Council and the IT Government Coordinating Council to better share information and coordinate activities;
- Educating and informing the Small and Medium Business (SMB) community about IT Sector threats, vulnerabilities, risks to the community, and the impact to critical infrastructure, and;
- Creating a best-practices document for the SMB community detailing NIST Cybersecurity Framework implementation.

Table 2-2*:* Examples of Partnership Engagements

Partnership Engagement	Activities and Meetings
SSA	•Participate in regular NIPP Working Group meetings •Participate in monthly Office of Infrastructure Protection (IP) SSA Coordination meetings •Attend quarterly IP Threat Information Sharing Framework Working Group meetings •Attend quarterly Federal Senior Leadership Council (FSLC) meetings
IT GCC	•Manage GCC-only Quarterly Meetings •Coordinate joint GCC-SCC bimonthly meetings •Attend annual IT SCC all-day coordination meeting
IT SCC	•Attend bimonthly IT SCC Executive Committee (EC) meetings with DHS/CS&C leadership •Attend bimonthly IT SCC EC meetings with IT GCC •Hold annual IT SCC meetings
Cross-Sector	•Hold annual, all-day IT and Communications Sectors Quad Meetings with both GCCs and SCCs •Conduct periodic Joint GCC meetings with Communications Sector •Participate in quarterly and biannual joint meetings for the Cross-Sector Councils •Participate in ad-hoc, cross-sector critical infrastructure meetings (e.g., Severe Weather Planning, Critical Aging Infrastructure, etc.)

State, Local, Tribal, and Territorial Governments

State and local governments provide IT services that fulfill the needs of their citizens, businesses, and employees. State governments engage in IT Sector activities through National Association of State Chief Information Officers' (NASCIO) participation in the IT GCC. Local governments engage in IT Sector

activities and the IT GCC through the State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC).

Table 2-3*:* Overview of SLTT IT Partners

Organization	Description
National Association of State Chief Information Officers (NASCIO)	An organization that represents senior IT leaders in each State and is a key partner of the IT Sector.
Multi-State Information Sharing and Analysis Center (MS-ISAC)	A collaborative organization, with participation from all 50 States, the District of Columbia, local governments, and U.S. Territories, that provides a common mechanism for raising the level of cybersecurity readiness and response for all participants.

International Organizations and Foreign Partners

The IT Sector is global, interconnected, and interdependent. As a result, international partners play a key role in the prevention, protection, response, and recovery of critical IT Sector functions. Establishing and maintaining consistent and reliable relationships with international partners is vital to ensuring the security of the Sector. Table 2-4 provides an overview of the private, public and joint Sector programs that support and promote international coordination and partnerships for the IT Sector. See Appendix B for a fuller description of each.

Table 2-4*:* Overview of International Private, Public, and Joint Sector Programs

Coordination Type	Program/Organization
Private Sector Coordination	Forum of Incident Response and Security Teams (FIRST)
	Network Service Provider Security forum (NSP-SEC)
	North American Network Operators' Group (NANOG)
	American Registry for Internet Numbers (ARIN)
	Internet Governance Forum (IGF)
	Internet Corporation for Assigned Names and Numbers (ICANN)
	Internet Engineering Task Force (IETF)
Public Sector Coordination	DHS Office of International Affairs Outreach and Awareness
	Multilateral Network Security Information Exchange
Joint Sector Coordination	DHS Critical Foreign Dependencies Initiative (CFDI)
	DHS Cyber Storm Exercises; FEMA National Level Exercises

3. Vision and Priorities

3.1 Sector Vision

The IT Sector provides an infrastructure upon which all other critical infrastructure Sectors rely. As such, the IT Sector's vision is:

"***To achieve a sustained reduction in the impact of incidents on the Sector's critical functions.***"

This vision supports:

- The Federal Government's performance of essential national security missions and preservation of general public health and safety;
- State and local governments' abilities to maintain order and deliver minimum essential public services; and,
- The orderly functioning of the economy.

3.2 Sector Priorities

As part of this 2016 SSP, the IT SCC and GCC have identified priorities to guide the Sector's security and resilience efforts over the next four years. The priorities include activities surrounding risk management, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, situational awareness, information sharing, and partnership and engagement. These efforts are conducted with the broader context of the global nature of IT Sector interests and activities.

In response to the NIPP 2013 Calls to Action[3], the national council structures worked collaboratively to establish joint national priorities. The call for joint national priorities was set forth in Call to Action #1: Set National Focus through Jointly Developed Priorities. Table 3-1 shows how the joint national priorities are aligned to the IT Sector joint priorities.

Table 3-1: Joint National Priorities and IT Sector Joint Priorities

Joint National Priorities	IT Sector Joint Priorities
Strengthen the Management of Cyber and Physical Risk to Critical Infrastructure	**Risk Management** – Identify, assess, and help facilitate the management of risks to the IT Sector's critical functions, including risks associated with supply chains, dependencies, and interdependencies, and facilitate joint understanding between industry and government of those risks.
	Cybersecurity Resilience – Better understand the public and private sector perspectives and initiatives of resilience (e.g., NIST Cybersecurity Framework).
Strengthen Collaboration across Sectors, Jurisdictions, and Disciplines	**Situational Awareness and Information Sharing** – Improve timely, actionable situational awareness for IT Sector partners through defined partnerships and

[3] U.S. Department of Homeland Security. NIPP 2013: Partnering for Critical Infrastructure Security and Resilience (2013). http://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience. Accessed November 19, 2015.

Joint National Priorities	IT Sector Joint Priorities
Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	mechanisms, such as the Information Technology Information Sharing and Analysis Center (IT-ISAC) and National Cybersecurity and Communications Integration Center (NCCIC), and working to implement the President's Executive Order "Promoting Private Sector Cybersecurity Information Sharing."
Build Capabilities and Coordination for Enhanced Incident Response and Recovery	**Partnership and Engagement** – Continue to improve the security and resilience of the IT Sector through collaborative public-private sector partnership, healthy institutions, and innovative risk management and resilience capabilities. Support and engage the IT-ISAC for Sector-wide and cross-sector operational incident response.
Enhance Effectiveness in Resilience Decision-Making	

4. Achieving Sector Goals

The IT Sector public-private partnership model enables partners to collaboratively identify threats and vulnerabilities to IT Sector critical functions and exchange mitigating and preventive tactics and resources to address them. Through continued public-private sector information sharing and enhanced cross-sector engagement, the IT Sector will be better prepared to:

- Shape critical infrastructure protection cybersecurity policy;
- Enhance the security and resilience of the critical IT Sector functions;
- Identify specific information each Sector partner wants to share, who needs it, and why and how to protect it;
- Improve public-private problem solving by deepening understanding of government and industry sector security requirements;
- Share and apply effective industry security practices, and;
- Assist in planning and developing DHS National Level Exercises to promote expeditious incident response capabilities.

The IT SCC has designated the IT-ISAC as the Sector's operational coordination point and, as such, provides a leadership role on cyber threat information sharing between the Sector and government and among other critical infrastructure Sectors.

4.1 Risk Management

4.1.1 Risk Management Approaches

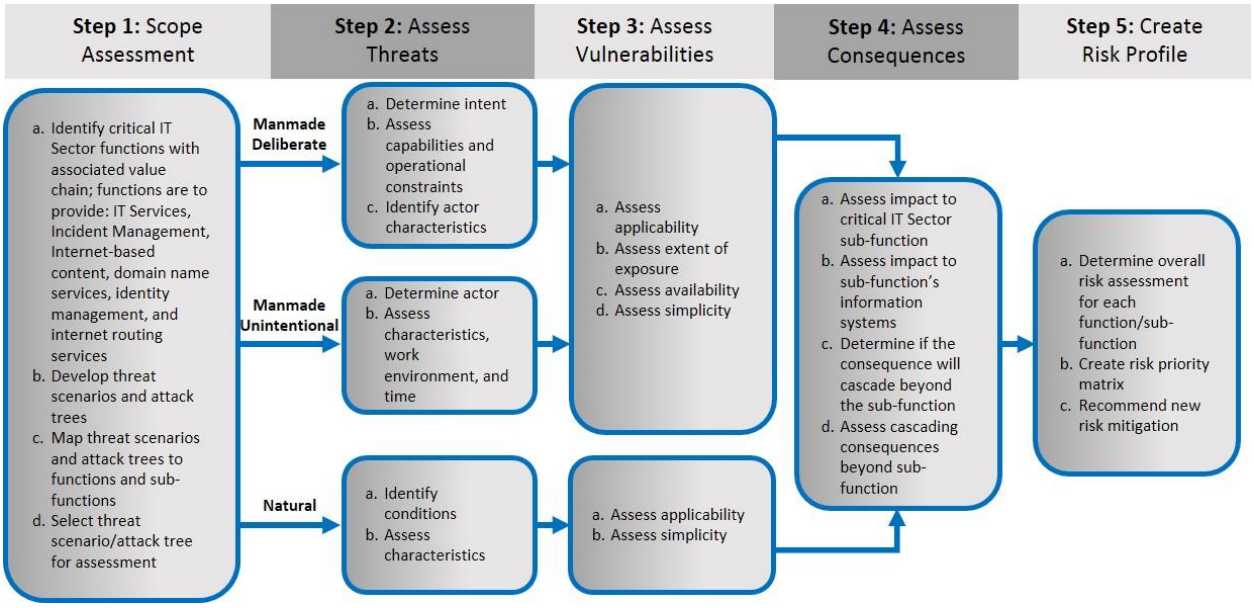
The IT Sector manages global operations that are interdependent and connected with other Sectors, many of which are international. In addition, the IT Sector is comprised of small, medium, and large companies that have varied levels of security resources and expertise. These operations face numerous multifaceted global threats from natural and manmade events. Many of these threats occur frequently, but do not have significant consequences because of individual entities' existing security and response capabilities. On the other hand, some of these threats are strategic and could affect critical functions and other elements of the Nation's critical infrastructure. The high degree of the IT Sector's interdependency, interconnectedness, and anonymity of actors makes identifying threats, assessing vulnerabilities, and estimating consequences at the national level difficult. For that reason, the IT Sector uses a collaborative and iterative risk management approach seeking to address the needs of its broad constituency and makeup.

All-Hazards Approach

The IT Sector has developed an all-hazards risk assessment methodology that applies a top-down, functions-based approach that considers the Sector's ability to support the economy and national security as part of the risk assessment's national-level scope. The purpose of utilizing a top-down approach is to identify functions that meet a minimum consequence threshold. Resources can then be devoted to analyzing and mitigating nationally consequential risks to the critical functions and their supporting infrastructure. Because the methodology takes an all-hazards approach, the Sector is able to link cyber and physical threats. Figure 4-1 provides a summary of the methodology used by subject matter experts to

assess risks to the critical functions.[4] The details that support each element and component of the methodology can be found in the IT Sector Risk Assessment Approach.[5]

Figure 4-1: IT Sector Risk Assessment Approach



The IT Sector uses its methodology and approach to evaluate risk across its critical functions and develop risk mitigation strategies for the risks of greatest concern. Creating awareness around the risk mitigation strategies allows the IT Sector to promote resilience to its stakeholders at the sector level.

Sector-wide and Enterprise Level Views

IT Sector risk management approach focuses on two levels: (1) the enterprise level and (2) the sector or national level. Private sector entities typically base their enterprise approaches on business objectives, such as shareholder value, efficacy, and customer service. Whereas, public sector entities usually base their enterprise approaches on ensuring mission effectiveness or providing a public service. Enterprise risk management approaches typically involve cybersecurity initiatives and practices to maintain the health of information security programs and infrastructures. Examples of these actions include physical vulnerability mitigation measures (e.g., physical access control and surveillance); human vulnerability mitigation measures (e.g., employee screening and security training and awareness); cybersecurity measures (e.g., encryption; behavior monitoring and management technologies; independent third-party security posture assessments); and business continuity planning. These individual risk management efforts are designed to support organizational objectives and, in the aggregate, they enhance the security and resilience of the IT Sector as a whole.

At the sector or national level, the IT Sector manages risk for its six critical functions (see Figure 2-1) to maintain information assurance and IT infrastructure resilience against cascading consequences of the Sector's interconnectedness and interdependencies. IT SCC and GCC partners determined that this top-

[4] The methodology leverages the knowledge and expertise of IT Sector partners, standards and guidance bodies, and other credible authorities in the IT, risk management, and critical infrastructure protection arenas.
[5] Information Technology Sector Baseline Risk Assessment, 2009. http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf. Accessed November 19, 2015.

down and functions-based approach, which focuses on understanding the functions of the infrastructure rather than cataloging physical fixed assets, is effective for the highly distributed infrastructure that enables entities to produce and provide IT hardware, software, and services. Additionally, the top-down approach enables public and private IT Sector partners to prioritize mitigation and protective measures to risks of national concern.

4.1.2 Risk Management Efforts

Overview

The IT Sector comprises not only physical assets but also virtual systems and networks that enable key capabilities and services in both public and private sectors. Even though the virtual nature of many IT systems provide additional resilience, the IT Sector understands the interconnectivity between cyber and physical security and recognizes the need for critical infrastructure owners and operators of all sizes to implement integrated cyber and physical security measures to enhance security and resilience within the sector. In order to identify and mitigate against both physical and cyber threats, the IT Sector engages in several different activities and programs, including the Cyber Storm Exercise Series, the Software and Supply Chain Assurance (SSCA) Working Group, and the IT Sector Risk Assessment (ITSRA). Section 5 of this document addresses how the IT Sector measures the success of its iniatives and details its joint priorities.

- Cyber Storm provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind. Congress mandated the Cyber Storm Exercise Series to strengthen cyber preparedness in the public and private sectors. Cyber Storm participants perform the following activities:
    - Examine organizations' capability to prepare for, protect from, and respond to the potential effects of cyberattacks;
    - Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
    - Validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information;
    - Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests; and
    - Each Cyber Storm builds on lessons learned from previous real world incidents, ensuring that participants face more sophisticated and challenging exercises every two years.
- The SSCA Working Group, co-sponsored by organizations within DHS, Department of Defense (DoD), NIST, and General Services Administration (GSA), brings together stakeholders responsible for protecting the Nation's key information technologies—most of which are enabled and controlled by software and influenced by external dependencies on the supply chain. The SSCA Working Group meets quarterly with the SSCA Forums meeting on a semi-annual basis in spring and fall, and the SSCA Working Groups (meeting in between Forums) in the summer and winter. The IT Sector (GCC and SCC members) attends and participates in the quarterly meetings. Some of the sessions or topic areas have included software lifecycle development, tools and resources for supply chain risk management, and industrial control system supply chain assurance.
- The ITSRA is intended to provide an all-hazards risk profile that IT Sector partners can use to inform resource allocation for research and development and other protective program measures to enhance the security and resilience of the critical IT Sector functions. By increasing the

awareness of risks across the public and private sector domains, the Baseline Risk Assessment serves as a foundation for ongoing national-level collaboration to enhance the security and resilience of the critical IT Sector functions.

Physical Risk Management Efforts

The IT Sector's physical infrastructure risks primarily encompass those that threaten public health or safety, undermine public confidence, have a negative effect on the national economy, or diminish the security posture of the Nation. Physical infrastructure risks also include natural disasters, such as earthquakes, floods, and hurricanes. When analyzing physical vulnerabilities, the sector's approach will assess the likelihood of a physical vulnerability for people, processes, or technology to exploit a resource.

If a physical threat is identified in the IT Sector, the primary points of coordination are the IT SSA and the National Infrastructure Coordinating Center (NICC). Additionally, the IT-ISAC provides another, primary front-line of coordination to help share and analyze strategic responses among the IT-ISAC members. The IT-ISAC serves as a central repository for security-related information about threats, vulnerabilities, and best practices related to physical and cyber events, and is responsible for the receipt and dissemination of this information to ISAC members.

Cybersecurity Risk Management Efforts

In addition to addressing physical infrastructure risks, the IT Sector also takes steps to improve its cybersecurity resilience. To guide these efforts, the IT Sector plans to align its activities with the NIST Cybersecurity Framework (the Framework). The Framework assists critical infrastructure sectors and organizations with mitigating and managing cyber risks.

Executive Order 13636 and NIST Cybersecurity Framework Implementation

To help engage all critical infrastructure Sectors with the Framework, Executive Order 13636 in 2013 created, in addition to the Framework, the Critical Infrastructure Cyber CommunityVoluntary Program (C^3VP). C^3VP encourages critical infrastructure owners and operators to establish or improve their cyber risk management processes and to take advantage of resources made available by the government. C^3VP supports the practical application of the Framework by facilitating access to free technical assistance, tools, and other resources to help critical infrastructure owners and operators strengthen their capacity to manage cyber risk

To encourage Framework use across the Sector, IT SSA is working to assist the government, industry, and sector partners with understanding use of the Framework and other risk management efforts. Additionally, the IT Sector looks to connect sector partners, interested companies, and organizations to DHS, public, and private sector resources to support use of the Framework.

Development of IT Sector Implementation Guidance

In 2016, the IT SSA will work with the C^3 Voluntary Program members to consider developing broader IT Sector NIST Cybersecurity Framework use guidance, created in partnership with the IT SCC. The guidance aims to grow an organization's understanding of:

- Framework terminology, concepts, and benefits;
- Existing Sector cybersecurity tools and resources that support Framework use by companies of all sizes;
- A common approach for using the Framework; and
- Suggestions for how to link organizational cyber risk management activities to their respective Sector.

As with the Framework itself, the guidance will apply to organizations of any size and level of cybersecurity sophistication. For organizations with no formal risk management practices, the guidance will provide the foundational principles and elements for building a program. For organizations with robust programs, it will provide a potential means to identify areas for improvement. The guidance is intended to provide a Sector with actions and resources to help understand and use the Framework, structured around the five core function areas of the Framework.

4.1.3 Research and Development Opportunities

For long-term mitigation and response planning, the IT Sector provides R&D recommendations and requirements to the Federal Government during joint IT SCC and GCC meetings in coordination with DHS Science and Technology Directorate. These R&D recommendations focus on critical function areas of the IT Sector. The IT Sector liaisons work to ensure that the Sector's R&D priorities align to the existing initiatives within the government.

Leveraging private sector R&D investment while respecting the proprietary nature of some of those efforts and sharing information on government R&D initiatives and priorities are critical to the IT Sector's overall R&D strategy. To understand the challenge of collaboration better in this environment, the IT Sector partners visualize the role of public and private sector R&D as an ecosystem where the private sector focuses on certain portions of R&D that are commercially viable.

As the IT Sector advances its R&D agenda, it will be important for the public and private sectors to work collaboratively and share R&D information in pursuit of Sector objectives. Moving forward, the IT Sector will need to continue coordination with the Communications Sector on R&D critical infrastructure protection priorities that overlap or have inherent synergies; share results from the collaborative framework with R&D public and private sector partners; and develop a roadmap for IT Sector R&D priorities and resource needs.

The Critical Infrastructure Security and Resilience National Research and Development Plan[6] (CISR National R&D Plan) required by PPD-21 was released in February 2015. It presents five overarching CISR National R&D Priority Areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure community.

The CISR National R&D Priority Areas are:

- Develop the foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk assessment and management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and
- Build a crosscutting culture of critical infrastructure security and resilience R&D collaboration.

The IT Sector will consider these five Priority Areas as inputs in its planning and coordination efforts to align its R&D activities and support implementation of the CISR National R&D Plan.

[6] Critical Infrastructure Security and Resilience National Research and Development Plan. http://www.dhs.gov/publication/cisr-national-rd-plan-final-report

4.2 Assessment of Future IT Sector Risks

From 2006 to the present, the IT Sector conducted a number of Sector-wide, functions-based risk assessments related to various aspects of the Sector's six critical functions. The Sector has discussed the following areas for future risk assessments:

- Developing metrics for cybersecurity services;
- Studying cloud risk topics;
- Measuring IT Sector risk management strategy effectiveness;
- Studying information sharing roles in IT Sector critical functions;
- Assessing consumer risks in moving to cloud environments, and;
- Assessing risks to digital certificate issuance and root authority.

See Appendix C for more on these risk management studies.

Supply Chain Risk Management

The assurance and integrity of IT Products and Services has become a critical issue within most types of organizations, and finding better ways to address the topic has become one of the IT Sector's joint priorities. Sharing and leveraging software assurance knowledge is becoming a key enabler to making the types of changes and improvements that are needed to address supply chain risk.

The IT Sector is heavily engaged with activities of the Software and Supply Chain Assurance (SSCA) Program DHS CS&C. The SSCA program promotes software and supply chain security and resilience via enhanced processes and diagnostics; enables public private collaboration focused on reducing exploitable software weaknesses and addressing means to improve capabilities that routinely develop, acquire, and deploy resilient software products. The SSCA Working Group sessions, held semiannually, provide venues for public-private collaboration in advancing software and supply chain assurance. These events bring together stakeholders responsible for protecting the Nation's key information technologies—most of which are enabled and controlled by software and influenced by the supply chain. Both government and industry representatives from the IT Sector are active participants in SSCA activities, working to develop recommendations and then incorporate initiatives into the IT Sector.

5. Measuring Effectiveness

5.1 Sector Initiatives

As previously discussed, the IT Sector developed a set of joint public and private sector priorities to help inform its efforts and to feed into the development of the Joint National Priorities. In working to achieve its priorities, as well as measuring and reporting effectiveness over time, the Sector will leverage the 2013 NIPP Calls to Action as categories to track and provide progress of Sector activities to DHS. The NIPP Calls to Action, established in the NIPP 2013, guides efforts to achieve national goals aimed at enhancing national critical infrastructure security and resilience. The NIPP Calls to Action will serve as a roadmap to ensure continuous improvement of security and resilience through the IT Sector efforts. The actions listed below provide strategic direction for national efforts in the coming years.

Build upon Partnership Efforts (1-4):

1. Set National Focus through Jointly Developed Priorities
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience

Innovate in Managing Risk (5-10):

5. Enable Risk-Informed Decision-Making through Enhanced Situational Awareness
6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by Advancing R&D Solutions

Focus on Outcomes (11-12):

11. Evaluate Progress toward the Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

Table 5-1 shows how the Sector's priorities and initiatives are aligned to the NIPP Calls to Action.

Table 5-1: Alignment of IT Sector Priorities and Initiatives with NIPP Calls to Action

Joint National Priorities	IT Sector Joint Priorities	2013 NIPP Calls to Action Mapping
Strengthen the Management of Cyber and Physical Risk to Critical Infrastructure	**Risk Management** – Identify, assess, and help facilitate the management of risks to the IT Sector's critical functions, including risks associated with supply chains, dependencies, and interdependencies, and facilitate joint understanding between industry and government of those risks.	Calls to Action 5-10: Innovate in Managing Risk Calls to Action 11-12: Focus on Outcomes
	Cybersecurity Framework – Better understand the implications of the NIST Cybersecurity Framework for the IT Sector.	Calls to Action 5-10: Innovate in Managing Risk
Strengthen Collaboration across Sectors, Jurisdictions, and Disciplines Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	**Situational Awareness and Information Sharing** – Improve timely, actionable situational awareness for IT Sector partners through defined partnerships and mechanisms, such as the IT-ISAC and NCCIC, and working to implement the President's Executive Order "Promoting Private Sector Cybersecurity Information Sharing."	Calls to Action 1-4: Build on Partnership Efforts Calls to Action 5-10: Innovate in Managing Risk Calls to Action 11-12: Focus on Outcomes
Build Capabilities and Coordination for Enhanced Incident Response and Recovery Enhance Effectiveness in Resilience Decision-Making	**Partnership and Engagement** – Continue to improve the security and resilience of the IT Sector through collaborative public-private sector partnership, healthy institutions, and innovative risk management and resilience capabilities.	Calls to Action 1-4: Build on Partnership Efforts

5.2 Measurement Approach

The IT SSA will have the primary responsibility for tracking and capturing sector-wide progress toward partnership activities using jointly developed metrics. The sector will leverage the NIPP Calls to Action[7] as categories to track and report quarterly on the progress of sector activities. Regular reports and data calls from DHS Office of Infrastructure Protection on the progress of these activities will demonstrate how the sector is collaboratively using the NIPP Calls to Action as strategic guidance for its activities over the coming years. The SSA will also be responsible for describing sector progress through the National Annual Reporting process, when updating the Sector-Specific Plan, and other possible channels.

The IT Sector is committed to pursuing the resilience and preparedness of the sector's critical infrastructure. As a result, the IT Sector is engaged in a number of security, preparedness and resilience activities to achieve the sector priorities and objectives reflected in the tables below. To reflect the evolution of cybersecurity threats and risks, the ITSSP is updated every four years. The IT Sector may modify the activities undertaken to support the objectives to reflect evolving risk, changes in prioritization, and progress or completion.

[7] NIPP 2013, pp. 21-26

Table 5-2: IT Sector Risk Management Activities

Joint Sector Priority: Risk Management		**NIPP Calls to Action** Calls to Action 5-10: Innovate in Managing Risk Calls to Action 11-12: Focus on Outcomes
Priority	Identify, assess, and help facilitate the management of risks to the IT Sector's critical functions, including risks associated with supply chains, dependencies, and interdependencies, and facilitate joint understanding between industry and government of those risks.	
Objectives	**Risk Assessments** — Periodically review and reassess risk to the IT Sector's critical functions, as well as conduct new assessments as need arises.	**Supply Chain Risk Management** — Contribute to initiatives intended to understand and enhance the assurance and integrity of IT products and services throughout their supply chains.
Activities	• Periodic reassessment of ITSRA critical functions and associated risks. • Root Authority Risk Assessment and cloud-based security. • Collaboratively contribute to the activities associated with Executive Order 13636, Section 9 related to annual identification of critical infrastructures at great risk. • Engage in SSCA Working Group to maintain awareness of, coordinate across, and, as appropriate, drive convergence among public and private sector efforts to help manage supply chain risks.	

Table 5-3: IT Sector Cybersecurity Framework Activities

Joint Sector Priority: Cybersecurity Framework	**NIPP Calls to Action** Calls to Action 5-10: Innovate in Managing Risk
Priority	Better understand cybersecurity resilience for the IT Sector.
Objectives	**Cybersecurity Resilience** – Better understand the public and private sector perspectives and initiatives of resilience (e.g., NIST Cybersecurity Framework).
Activities	• Use findings from Intel Corporation's pilot program, designed using the NIST Framework to improve their cyber security standards and awareness, as a baseline for other private sector efforts if needed. • Conduct twice annual qualitative feedback request of IT SCC member organizations' and entities' participation in or engagement with the Cybersecurity Framework. • Develop NIST Cybersecurity Framework reference for IT Sector entities. • Provide collective input into efforts related to NIST Framework Roadmap.

Table 5-4: IT Sector Situational Awareness and Information Sharing Activities

Joint Sector Priority: Situational Awareness and Information Sharing		**NIPP Calls to Action** Calls to Action 1-4: Build on Partnership Efforts Calls to Action 5-10: Innovate in Managing Risk Calls to Action 11-12: Focus on Outcomes
Priority	Improve timely, actionable situational awareness for IT Sector partners through defined partnership and mechanisms, such as the IT-ISAC and the NCCIC.	
Objective	**Operational Sharing** – Identify needs and address barriers to IT Sector information sharing by leveraging existing IT Sector entities, such as the IT-ISAC, to improve exchange of tactical and technical risks among IT Sector partners. Utilizing the IT-ISAC in this manner will complement its role as the operational arm of the IT SCC.	
Activities	• Continue to work through the IT-ISAC to determine how to enhance operational information sharing.	

Table 5-5: IT Sector Partnership and Engagement Activities

Joint Sector Priority: Partnership and Engagement		**NIPP Calls to Action** Calls to Action 1-4: Build on Partnership Efforts
Priority	Continue to improve the security and resilience of the IT Sector through collaborative public-private sector partnership, healthy institutions, and innovative risk management and resilience capabilities.	
Objectives	**Internal Partnerships** – Institutionalize and innovate effective structures and processes within the IT SCC and IT GCC to better share information and coordinate activities.	**External Engagement** – Institutionalize and innovate effective structures and processes between the IT SCC, the IT GCC, U.S. Government, and other critical infrastructure partnership to enhance security and resilience both domestically and internationally.
Activities	• Develop joint IT Sector priorities and review and discuss quarterly activities underway or planned that align with these priorities. • Identify joint risk priorities shared by the Communications and IT Sectors that can offer unique points of view on perceived dependencies or interdependencies and best practices. • Provide IT Sector inputs to cross-sector information sharing and special initiatives in bodies, such as the Cross-Sector Cyber Security Working Group (CSCSWG), and ensure IT government and industry views are represented in positions, materials, and recommendations, including the development of cybersecurity incentives. • Hold an annual IT and Communications Sectors Quad meeting and ensure sector priorities and efforts are communicated between sectors and government partners. • Identify a set of clear near- and long-term actions that the public and private sectors can take to have a stronger and more unified voice on internationally relevant issues related to Communications and IT Sector priorities. • Describe the discussions and activities occurring across various sectors using the Framework. • Discuss ways in which Communications and IT Sector companies are engaging or being affected by the audit and insurance communities that may lead to risk reduction. • Identify and discuss ways in which the sectors and SCCs can encourage better risk management through use of the Framework or other best practices. • Follow and promote throughout the Federal Government the partnership principles developed by the Partnership for Critical Infrastructure Security (PCIS) and accepted by IP.	

The IT Sector will continue to regularly evaluate its priorities, objectives, and activities and use identified sector metrics to capture outcomes and success stories.

Appendix A: IT Sector GCC and SCC Members

A-1: IT Government Coordinating Council Members

Department of Commerce

Department of Defense

Department of Energy

Department of Homeland Security

- National Protection and Programs Directorate (NPPD)
  - Office of Cybersecurity & Communications
  - Office of Infrastructure Protection
- Office of Intelligence & Analysis
- Science and Technology Directorate
- Transportation Security Administration

Department of the Interior

Department of Justice

Department of State

Department of the Treasury

Federal Bureau of Investigation

General Services Administration

National Association of State Chief Information Officers

National Institute of Standards and Technology

State, Local, Tribal, and Territorial Government Coordinating Council

A-2: IT Sector Coordinating Council Members

Adobe Systems Incorporated

Advanced Micro Devices (AMD)

Afilias USA, Inc.

Araxid

Aveshka

Bell Canada

Biofarma

Bivio Networks

Blackberry

BSA-The Software Alliance

Center for Internet Security

Certichron Inc

Cisco Systems, Inc.

Coal Fire Systems

CA Technologies
Computer Sciences Corporation
CompTIA
Core Security Technologies
Cyber Pack Ventures Inc.
Dell
Deloitte & Touche LLP
Dunrath Capital
Dynetics, Inc.
e-Management
Ebay
Echelon One
EMC Corporation
Entrust, Inc.
Equifax, Inc.
EWA Information & Infrastructure Technologies, Inc.
Exelis, Inc.
FireEye
Green Hills Software
Google
Hatha Systems
HP
IBM Corporation
Intel Corporation
Information Technology- Certification and Security Experts (ISC2)
Information Technology Industry Council (ITI)
Information Technology - Information Sharing & Analysis Center (IT-ISAC)
Internet Security Alliance
iWire365, Inc.
ITT Exelis
Juniper Networks
KPMG LLP
Kwictech
L-3 Communications
Lancope, Inc
Litmus Logic

LGS Innovations
Lockheed Martin
Lumeta Corporation
Lunar Line
Microsoft Corporation
Motorola
NetStar-1
Neustar
Northrop Grumman
NTT America
One Enterprise Consulting Group, LLC
Pragmatics
Rackspace Hosting
Raytheon
Reclamere
Renesys Corporation
SAIC
SafeNet Government Solutions
Seagate Technology
SecureState
Sentar Inc
Serco
The SI Organization
Siemens Healthcare
Sony
Symantec Corporation
System 1
TASC Incorporated
Telecom Industry Association (TIA)
Team Cymru
Telecontinuity, Inc.
Terremark World Wide
TestPros, Inc.
Triumfant
Tyco
U.S. Internet Service Provider Association

Unisys Corporation
Vanguard
VeriSign
Verizon
VOSTROM
Xerox

Appendix B: IT Sector International Organizations and Partners

Table B-1: IT Sector International Organizations and Partners

Coordination Type	Program/Organization	Description
Private Sector Coordination	Forum of Incident Response and Security Teams (FIRST)	Security incident response teams from government, commercial, and educational organizations to enable incident response teams to respond both reactively and proactively to security incidents
	Network Service Provider Security forum (NSP-SEC)	A volunteer incident response mailing list that coordinates the interaction between ISPs and Network Service Providers (NSPs) in near-real time, tracks exploits and compromised systems, and mitigates the effects of exploits on ISP networks.
	North American Network Operators' Group (NANOG)	A forum for coordination and dissemination of technical information on the network backbone and operations.
	American Registry for Internet Numbers (ARIN)	Manages IP allocation for the United States, Mexico, Canada, and the Caribbean.
	Internet Governance Forum (IGF)	A multi-stakeholder dialog on public policy related to Internet governance issues convened under the auspices of the United Nations.
	Internet Corporation for Assigned Names and Numbers (ICANN)	A nonprofit organization that coordinates the domain name and addressing system.
	Internet Engineering Task Force (IETF)	International organization that develops Internet standards and protocols.
	The Information Technology - Information Sharing and Analysis Center (IT-ISAC)	A unique and specialized forum for managing risks to their corporations and the IT infrastructure. Members participate in national and homeland security efforts to strengthen the IT infrastructure through cyber information sharing and analysis.

Coordination Type	Program/Organization	Description
Public Sector Coordination	DHS Office of International Affairs Outreach and Awareness	Conducts international outreach and facilitates collaboration, cooperation, planning, and policy development on global cybersecurity issues.
	Multilateral Network Security Information Exchange	The U.S. NSIEs join with their counterparts from Australia, Canada, New Zealand and the U.K. at Multilateral NSIE Meetings, which are held every 14-18 months.
Joint Sector Coordination	DHS Critical Foreign Dependencies Initiative (CFDI)	Extends the sector's protection strategy overseas to include important foreign infrastructure that, if attacked or destroyed, could critically impact the United States.
	Cyber Storm Exercise	A DHS sponsored biennial exercise series to assess and strengthen cyber preparedness; examine incident response processes in response to ever-evolving threats; and enhance information sharing among Federal, State, international, and private sector partners.

Appendix C: IT Sector Risk Assessment Activities

Cloud Risk Topics for Future Assessment

Activity Type: Issue Study
Participants: IT GCC
Description: When the IT Sector began scoping a potential cloud-based services risk assessment, several risk experts suggested conducting a pilot assessment to determine if the agreed-upon approach is sufficient. Through this issue study, IT GCC participants will identify cloud risk topics and frame them for future assessment with IT SCC partners. In addition to identifying risk topics for assessment, this study will provide a suggested approach the IT Sector can take for assessing these risk topics within the framework of the ITSRA IT Sector functions. To inform this effort, the Industry Engagement and Resilience Branch within the Office of Cybersecurity and Communications will engage Federal partners, industry partnerships, and related organizations, such as the Cloud Security Alliance, to provide the most comprehensive cloud risk perspective possible.

IT Sector Risk Mitigation Strategy Effectiveness

Activity Type: Risk Management Plan
Participants: IT GCC and SCC
Description: Since the IT Sector completed the IT Sector Baseline Risk Assessment (ITSRA) in 2009, risk mitigation strategies have been developed for each of the sector's six critical functions. However, the effectiveness of those mitigation strategies has not been assessed. Through this activity, participants will determine the status of those mitigations and evaluate their effectiveness. Additionally, they will document how the IT Sector identifies risks, develops mitigation strategies, and implements these strategies on a sector level. Feedback will be solicited from both public and private sector partners to provide a comprehensive overview of the sector's approach to risk assessment and mitigation.

Information Sharing Roles in IT Sector Critical Functions

Activity Type: Issue Study
Participants: IT GCC and SCC
Description: Interest in the role information sharing plays in resilience and risk mitigation has increased, culminating in the signing of an Executive Action aimed at improving information-sharing efforts. Through this study, the IT Sector will examine the role information sharing plays in the provision of the sector's critical functions, specifically the Incident Management critical function where timely and accurate information sharing is vital. This study will consider information-sharing requirements in steady state and incident response scenarios to determine if current and proposed information-sharing mechanisms are adequate. A list of recommendations will be developed for consideration by IT and cross-sector partners.

Consumer Risk in Moving to Cloud Environments

Activity Type: Risk Assessment
Participants: IT GCC

Description: Cloud service providers (CSP) assume and mitigate many risks associated with the provision of cloud services. Consumers may assume some risks during implementation (e.g., establishing security requirements), but they also face risks related to ongoing use (e.g., security alert processes, IT governance, and reliable controls). Consumers may not have a good understanding of these implementation and usage risks.

Through this activity, IT GCC partners will assess the risks associated with cloud-based services from a consumer's perspective. To provide a consistent reference for potential risk areas, the Cybersecurity Framework's core functions and categories will shape the assessment. The findings of this risk assessment will be presented to IT SCC risk partners for consideration and will complement the assessment of cloud risks from a provider perspective; an assessment that would need to be led by the SCC. Once complete, the IT GCC and SCC will partner to identify and assess the risks that fall between consumers and providers.

Digital Certificate Issuance and Root Authority

Activity Type: Risk Assessment
Participants: IT GCC and SCC
Description: This activity was originally included as the third in a series of risk assessments to be conducted over 2014-2015 beginning with an assessment of the DNS and Internet Routing critical functions. This assessment will focus on risk considerations associated with digital certificate issuance and root authority. The assessment will primarily focus on the Provide Identity Management and Associated Trust Support Services critical function; however, there may be other critical function elements that play a role in digital certificate issuance and root authority.

Appendix D: Relevant Authorities

This key-authorities appendix provides a brief description of major authorities as they relate to IT Sector critical infrastructure security and resilience activities.

Homeland and National Security Authorities

Executive Order (EO) 13691, Promoting Private Sector Information Sharing (February 2015): President Obama issued an Executive Order directing the Department of Homeland Security (DHS) to encourage the development of information sharing and analysis organizations (ISAOs). To keep pace, all types of organizations, including those beyond traditional critical infrastructure sectors, need to be able to share and respond to cyber risk in as close to real-time as possible. Organizations engaged in information sharing related to cybersecurity risks and incidents play an invaluable role in the collective cybersecurity of the United States.

National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience (NIPP 2013) (February 2013): In February 2013, the President issued Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience, which explicitly calls for an update to the NIPP. The NIPP 2013 is informed by significant evolution in the critical infrastructure risk, policy, and operating environments, as well as experience gained and lessons learned since the NIPP issued in 2009. The NIPP 2013 builds upon previous NIPPs by emphasizing the complementary goals of security and resilience for critical infrastructure. To achieve these goals, cyber and physical security and the resilience of critical infrastructure assets, systems, and networks are integrated into an enterprise approach to risk management. The NIPP 2013 guides the national effort to manage risk to the Nation's critical infrastructure.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity (February 2013): This EO directs the Executive Branch to develop a technology-neutral voluntary cybersecurity framework; promote and incentivize the adoption of cybersecurity practices; increase the volume, timeliness, and quality of cyber threat information sharing; incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure; and explore the use of existing regulation to promote cybersecurity.

Presidential Policy Directive 21 (PPD-21), Critical Infrastructure Security and Resilience (February 2013): This directive, which replaces Homeland Security Presidential Directive (HSPD) 7, directs the Executive Branch to develop a situational awareness capability that addresses both physical and cyber aspects of how infrastructure is functioning in near-real time, understand the cascading consequences of infrastructure failures, evaluate and mature the public-private partnership, update the National Infrastructure Protection Plan, and develop comprehensive research and development plan.

Presidential Policy Directive 8 (PPD-8), National Preparedness (March 2011): This directive aims to strengthen the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk to the security of the nation, including acts of terrorism, cyberattacks, pandemics, and catastrophic natural disasters.

Export Administration Act of 1979, as amended (EAA), implemented through the Export Administration Regulations (August 2006): The EAA authorizes the Secretary of Commerce to regulate exports of commodities, software, and technology (collectively referred to as "items") based on

national security and foreign policy objectives. Under the EAA, controls are placed on export of items based on their technical capabilities and the destination. The EAA currently is lapsed, but the Export Administration Regulations remain in effect through the International Emergency Economic Powers Act (described below), Executive Order 13222, and the Presidential Notice of August 3, 2006.

Presidential Memorandum for the Heads of Executive Departments and Agencies: Guidelines and Requirements in Support of the Information-Sharing Environment (December 2005): This Presidential memorandum outlines information-sharing authorities and directs executive departments and agencies, in consultation with the program manager for information sharing, to leverage ongoing information-sharing efforts in development of the Information-Sharing Environment (ISE) and to promote a culture of information sharing. In addition, this memorandum provides guidelines for the ISE: define common standards for how information is acquired, accessed, shared, and used in the ISE; develop a common framework for sharing information between and among executive departments and agencies and State, local, and tribal governments, law enforcement agencies, and the private sector; standardize procedures for Sensitive but Unclassified (SBU) information; facilitate information sharing between executive departments and agencies and foreign partners; and protect the information privacy rights and other legal rights of Americans.

Intelligence Reform and Terrorism Prevention Act of 2004 (December 2004): This act represents the most dramatic reform to the Nation's intelligence capabilities since the National Security Act of 1947. This authority requires the President to establish an ISE to facilitate sharing terrorism information among all appropriate Federal, State, regional, local, and tribal government and private sector entities through the use of policy guidelines and technologies; to include provisions for privacy and civil liberty rights; to establish programs for the enhancement of public safety communications interoperability; and to recommend that DHS promote the adoption of voluntary national preparedness standards for the private sector. The act and its subsequent authorization legislation established the position of Director of National Intelligence (DNI) and gave the DNI and DNI/Chief Information Officer (CIO) significant additional authorities and responsibilities for the management of the intelligence community and its role in critical infrastructure protection.

HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors (August 2004): This directive establishes national policy to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). "Secure and reliable forms of identification" in this directive means identification that: (1) is issued based on sound criteria for verifying an individual employee's identity; (2) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (3) can be rapidly authenticated electronically; and (4) is issued only by providers whose reliability has been established by an official accreditation process. IT Sector technologies and infrastructure facilitate the implementation of this directive, and future developments in the sector can affect efforts to maintain the common identification standard.

HSPD-9, Bio Defense Strategy (April 2004): This directive establishes national policy that prioritizes the protection of critical infrastructure (physical and cyber) from the effects of biological weapons attacks. A biological weapons attack might deny access to essential facilities and response capabilities; therefore, it is necessary to improve the survivability and ensure the continuity and restoration of operations of critical infrastructure sectors following biological weapons attacks. Assessing the vulnerability of this infrastructure—particularly, the medical, public health, food and agriculture, water, energy, and transportation sectors—is the focus of current efforts. DHS, in coordination with other

appropriate Federal departments and agencies, leads these efforts, which include developing and deploying bio-detection technologies and decontamination methodologies. This HSPD is relevant because human elements of critical IT Sector functions exist. If this human element were affected by a biological attack, cascading effects might occur. For example, if an antivirus vendor organization's campus were affected, the skills and knowledge needed to perform virus definition updates and patching potentially might be unavailable during a crucial time.

HSPD-8, National Preparedness (December 2003): This directive establishes policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, regional, local, and tribal entities.

The Homeland Security Act of 2002 (November 2002): The Homeland Security Act established the following specific critical infrastructure protection roles and responsibilities for DHS:

- Developing a comprehensive national plan for securing the critical infrastructure of the United States;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities on emergency recovery plans for failures of critical information systems; and
- Coordinating with other agencies of the Federal Government to provide specific warning information and advice about appropriate protective measures and countermeasures to State, local, and nongovernment organizations.

Exon-Florio Amendment to the Defense Production Act and Executive Orders 11858, 12188, and 12661 (May 1975, January 1980, and December 1988): These provisions authorized the creation of the Committee on Foreign Investment in the United States (CFIUS), which is an interagency committee chaired by the Department of the Treasury. The mission of CFIUS is to review and potentially recommend that the President block foreign acquisitions of U.S. companies that threaten to impair national security.

National Strategies

Federal Information Security Modernization Act (FISMA) (December 2014): FISMA 2014 codifies the Department of Homeland's Security's role in administering the implementation of information security policies for Federal Executive Branch civilian agencies, overseeing agencies' compliance with those policies, and assisting Office of Management and Budget (OMB) in developing the policies. The legislation provides the Department authority to develop and oversee the implementation of binding operational directives to other agencies. FISMA 2014 also:

- Authorizes DHS to provide operational and technical assistance to other Federal Executive Branch civilian agencies at the agency's request;
- Places the Federal information security incident center (a function fulfilled by United States Computer Emergency Readiness Team (US-CERT)) within DHS by law;
- Authorizes DHS technology deployments to other agencies' networks (upon those agencies' request);
- Directs OMB to revise policies regarding notification of individuals affected by Federal agency data breaches;

- Requires agencies to report major information security incidents as well as data breaches to Congress, as they occur and annually; and
- Simplifies existing FISMA reporting to eliminate inefficient or wasteful reporting, while adding new reporting requirements for major information security incidents.

The Federal Information Security Amendments Act of 2012 (April 2012): This act enhances the Federal Information Security Management Act (FISMA) of 2002 by improving the framework for ensuring security over information technology systems that support the Federal Government. It establishes a mechanism for stronger oversight through a focus on automated and continuous monitoring of cybersecurity threats and conducting regular threat assessments.

The National Strategy for Homeland Security (October 2007): The National Strategy for Homeland Security provides a four-goal framework for national homeland security efforts:

- Prevent and disrupt terrorist attacks;
- Protect the American people, our critical infrastructure, and key resources;
- Respond to and recover from incidents that do occur; and
- Continue to strengthen the foundation to ensure our long-term success.

The strategy focuses on terrorist threats as well as the full range of potential catastrophic events, including manmade and natural disasters, due to their implications for homeland security. As noted within the Strategy, many of the Nation's essential and emergency services, as well as our critical infrastructure, rely on the uninterrupted use of the Internet and the communications systems, data, monitoring, and control systems that comprise our cyber infrastructure. A cyberattack could be debilitating to our highly interdependent critical infrastructure and key resources (CIKR) and, ultimately, to our economy and national security. DHS and its private sector partners are working within the NIPP framework to enhance the Nation's ability to respond in the event of an attack or major cyber incident.

Federal Acquisition Regulation, Part 39, Acquisition of Information Technology (February 2006): This regulation establishes acquisition policies and procedures for acquiring information and IT (excluding national security systems).

National Counterintelligence Strategy (March 2005): This strategy seeks to ensure that industry is not disadvantaged by foreign intelligence operations and provides appropriate threat information to industry and IT security partners to take appropriate risk mitigation measures. The strategy recognizes that the U.S. strategic response to today's threats requires that the Nation's counterintelligence capabilities need to address technical, cyber, and human threats.

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003): This national strategy outlines strategic objectives to identify and assure the physical protection of critical infrastructure and assets; provide timely warning of specific, imminent threats; assure protection of identified infrastructures and assets that face a threat; and assure the protection of infrastructures and assets that may become targets over time by pursuing specific initiatives and enabling a collaborative environment between the public and private sector.

Executive Order (EO) 13011, Federal Information Technology (January 2003): This EO outlines a coordinated IT approach that builds on current structures and successful practices to improve Federal Government mission performance and service delivery. It establishes the CIO Council, Government Information Technology Services Board, and Information Technology Resources Board to advise the President in carrying out the responsibilities of the Clinger-Cohen Act.

Federal Information Security Management Act (FISMA) of 2002 (November 2002): This act establishes a framework for the security of the Federal Government's IT by mandating annual audits of Federal Government entities and organizations affiliated with the Federal Government.

The National Strategy to Secure Cyberspace (July 2002): This strategy states that a top priority for the Nation is to understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications. The strategy directs DHS to work with State and local governments to establish strong IT security programs. It also describes the National Cyberspace Security Response System.

E-Government Act of 2002 (January 2002): This act improves electronic Federal Government processes and services promotion and management through the establishment of a Federal CIO at OMB. The act establishes a measurement framework that requires using Internet-based IT to help citizens gain better access to services and information.

Management and Acquisition of Federal Government Information Technology, Clinger-Cohen Act of 1996 (also known as the Information Technology Management Reform Act) (February 1996): Recognizing the importance of IT for effective government, Congress and the President enacted the Information Technology Management Reform Act and the Federal Acquisition Reform Act. These two acts, together known as the Clinger-Cohen Act, require the heads of Federal agencies to link IT investments to agency accomplishments. The Clinger-Cohen Act also requires that agency heads establish a process to select, manage, and control their IT investments. This act also reformed the way the Federal Government acquires and manages IT through performance-based and results-based management. The law focuses on IT investment management, information resources management, and IT management. It also directs all Federal agencies to use a formal enterprise architecture process. It transferred IT responsibilities from the General Services Administration (GSA) to OMB and further defined the role of an agency's CIO.

The Paperwork Reduction Act of 1995 (May 1995): This act establishes that the OMB Director will develop and oversee the "implementation of policies, principles, standards, and guidelines for information technology functions and activities of the Federal Government" to help enhance agency mission performance.

Information Technology Audit-Related Authorities

Defense Production Act of 1950, as amended (DPA) (October 2009): This act authorizes the President to, among other things, demand that companies accept and give priority to Federal Government contracts that the President "deems necessary or appropriate to promote the national defense." In 2003, the DPA was amended, so that the term "national defense" includes "critical infrastructure protection and restoration." The act authorizes the provision of financial incentives for certain technological development and domestic production.

National Response Framework (January 2008): Emergency Support Function (ESF) #2, Communications, coordinates Federal actions to support temporary national security and emergency preparedness (NS/EP) telecommunications and telecommunications infrastructure restoration. During response efforts, ESF #2 supports all Federal departments and agencies in the procurement and coordination of all NS/EP telecommunications services from the telecommunications and IT industry. The Cyber Security Incident Annex outlines policies, responsibilities, organization, and actions so that the Nation can prepare for, respond to, and recover from nationally significant events related to cyber.

Sarbanes-Oxley Act (SOX) of 2002 (July 2002): This act establishes policies related to corporate governance, the practice of public accounting, and financial disclosure. Section 404 largely affects every company's IT department as it outlines processes for addressing such things as installation of new business applications, application monitoring, and IT system and network security.

The Cyber Security Enhancement Act of 2002 (February 2002): The Cyber Security Enhancement Act of 2002 amends Federal computer crime sentencing guidelines, making it possible to issue more appropriate sentences for crimes involving fraud in connection with computers and access to protected information, protected computers, restricted data in interstate or foreign commerce, or involving a computer used by or for the Federal Government.

Health Insurance Portability and Accountability Act (HIPAA) (August 1996): Seeks to enhance health insurance coverage portability and continuity; stop health insurance and health care delivery waste, fraud, and abuse; foster medical savings accounts; increase long-term care services and coverage access; and make health insurance administration less complicated. The HIPAA Security Rule establishes minimum standards that safeguard electronic protected health information.

The Computer Fraud and Abuse Act of 1984 as amended by the Computer Abuse Amendments Act of 1994 (September 1994): Note: Section 1030 was amended on October 26, 2001, by the USA PATRIOT antiterrorism legislation. Section 1030: Fraud and related activity in connection with computers states that whoever, having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the U.S. Government pursuant to an executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph (y) of Section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation, willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit, or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it.

Information Technology Privacy Authorities and Information Protection Related Authorities
Electronic Communications Privacy Act (ECPA) (October 1986): This act establishes policies for access, interception, use, disclosure, and privacy protection of electronic communications for wire and electronic communications. ECPA prevents the Federal Government from mandating electronic communications disclosure without appropriate procedure.

The National Information Infrastructure Protection Act (October 1996): This act defines "protected information" as "information that has been determined by the U.S. Government pursuant to an EO or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data.

Appendix E: List of Acronyms and Abbreviations

ARIN	American Registry for Internet Numbers
BYOD	Bring Your Own Device
C³VP	Critical Infrastructure Cyber Community Voluntary Program
CFDI	Critical Foreign Dependencies Initiative
CFIUS	Committee on Foreign Investment in the United States
CIO	Chief Information Officer
CS&C	DHS Office of Cybersecurity and Communications
CSCSWG	Cross-Sector Cyber Security Working Group
CSP	Cloud Service Providers
CtA	NIPP Call to Action
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DNS	Domain Name System
DoD	Department of Defense
DOJ	Department of Justice
DPA	Defense Production Act
ECPA	Electronic Communications Privacy Act
EO	Executive Order
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FSLC	Federal Senior Leadership Council
GCC	Government Coordinating Council
GSA	General Services Administration
gTLD	generic Top Level Domain
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICANN	International Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum

IoT	Internet of Things
IP	DHS Office of Infrastructure Protection
ISE	Information-Sharing Environment
ISP	Internet Service Provider
IT	Information Technology
IT-ISAC	Information Technology Information Sharing and Analysis Center
ITSRA	Information Technology Sector Risk Assessment
JNP	Joint National Priority
MS-ISAC	Multi-State Information Sharing and Analysis Center
NANOG	North American Network Operators' Group
NASCIO	National Association of State Chief Information Officers
NCCIC	National Cybersecurity and Communications Integration Center
NICC	National Incident Coordinating Center
NIPP 2013	National Infrastructure Protection Plan 2013
NIST	National Institute of Standards and Technology
NPPD	DHS National Protection and Programs Directorate
NS/EP	National Security and Emergency Preparedness
NSIE	Network Security Information Exchanges
NSP	Network Service Provider
NSP-SEC	Network Service Provider Security forum
NSTAC	National Security Telecommunications Advisory Committee
OMB	Office of Management and Budget
PCIS	Partnership for Critical Infrastructure Security
PPD	Presidential Policy Directive
R&D	Research and Development
S&T	DHS Science and Technology
SAR	Sector Annual Report
SBU	Sensitive But Unclassified
SCC	Sector Coordinating Council
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SMB	Small and Medium Business
SOX	Sarbanes-Oxley Act
SSA	Sector-Specific Agency
SSCA	Software and Supply Chain Assurance
SSP	Sector-Specific Plan
TLD	Top-Level Domain

U.S.	United States
US-CERT	United States Computer Emergency Readiness Team