THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on the Internet of Things

DATE: TBD

DRAFT

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The rapid adoption of smart, adaptive, and connected devices—the "Internet of Things" (IoT)—is occurring across virtually all critical infrastructure sectors. Moreover, this is happening at a speed that far outpaces earlier technological developments. The IoT will bring significant societal benefits, many of which are already being realized through increased efficiencies, early detection of faults, improved reliability and resilience, and more. But the rapid and massive connection of these devices also brings with it risks, including new attack vectors, new vulnerabilities, and perhaps most concerning of all, a vastly increased ability to use remote access to cause physical destruction.

There is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.

Recognizing this, the Executive Office of the President, specifically the National Security Council, tasked the President's National Security Telecommunications Advisory Committee (NSTAC) to examine the cybersecurity implications of the IoT within the context of national security and emergency preparedness (NS/EP). The NSTAC found that IoT adoption will increase in both speed and scope, and that it will impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally, the NSTAC determined that there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.

Scope of the Study

In February 2014, the NSTAC issued the *Industrial Internet Scoping Report*, which summarized the work of the NSTAC's Industrial Internet Scoping Subcommittee. The report revealed that in addition to Industrial Internet, IoT is referred to by several terms, including machine-to-machine communications, Internet of Everything, and cyber-physical systems. In its report, the NSTAC described the IoT as an expansion of the global infrastructure through existing and evolving interoperable information and communication technologies that incorporates the interconnection of physical and virtual systems to enable new and automated capabilities. It also noted that the potential benefits of the IoT include the development of innovative services and, in many cases, more efficient use of infrastructure. However, it also found that the IoT has several security factors that Government and industry should consider, including an exponential expansion in attack surfaces, a changing threat landscape, privacy concerns, an increased potential for kinetic-focused cyber attacks, and changes to the hardware lifecycle. The NSTAC concluded that these benefits and risks were already being recognized in the early deployment of IoT, thus necessitating a better understanding of the technology, the implications of existing and new policy structures, and the impacts on critical infrastructure security and resilience. Following this examination, the NSTAC established the IoT Research Subcommittee (IoTS) to study the cybersecurity implications of the IoT, within the context of NS/EP.[1]

[1] IoT-enabled consumer products and services are out of scope for this report, except to the extent that they interact with NS/EP systems.

Summary of the Report

In 2008, the U.S. National Intelligence Council warned that the IoT would be a disruptive technology by 2025.[2] The Council said that individuals, businesses, and governments were unprepared for a possible future when network interfaces reside in everyday things. Almost six years later, this warning remains valid, though it now seems certain that the IoT will be disruptive far sooner than 2025—if it is not so already. The number of Internet-connected devices first outnumbered the human population in 2008, and that number continues to increase. By 2013, there were as many as 13 billion Internet-connected devices, and projections indicate that this will grow to 50 billion or more by 2020, generating global revenues of more than $8 trillion by 2020.[3] The pace of deployment led the NSTAC to conclude that there are only three years—and certainly no more than five—to influence how IoT is adopted. By 2020, there will be tens of billions of devices in use. Now is the time to influence how those devices are designed and what protocols govern their use; after they are deployed, new policy will only affect change at the margins.

In 2008 the National Intelligence Council warned the IoT would be a disruptive technology by 2025; six years later, it is clear that this will happen much sooner, if it has not already.

The IoT's deployment will have a direct impact on the Nation's NS/EP. Billions of IoT devices (e.g., sensors, processors, actuators) that can communicate with one another are being incorporated directly into the Nation's critical infrastructure systems. Many of these devices will be controlled remotely, often across the public Internet and from personal smartphones or tablets. Consumer devices will undoubtedly connect to networks that may have connectivity to critical systems, which will create new attack venues for an adversary. These venues will be particularly hard to defend because they may not be discovered until a malicious actor tries to exploit them. Finally, as the IoT evolves, it is possible—if not likely—that hardware and software used in the consumer market will later be used to develop devices that are integrated into critical systems.

The IoT will impact NS/EP as billions of devices are deployed with the potential to be connected remotely with many of the Nation's critical infrastructure systems.

Concerns regarding the IoT's deployment may be analogous to the development of the Internet and the cybersecurity problems the Nation currently faces. When the protocols that govern the Internet were developed, security was not a significant consideration. At the time, the pervasive use of the Internet—for everything from commerce to global communications to life-sustaining functions—was not conceivable; had early designers envisioned this, there would have been a higher priority on security. Today, the Nation stands on the edge of a similar revolution in how it interacts with devices and how the devices will serve the country; however, if we do not include security as a core consideration, there will be significant consequences to both national and economic security.

[2] National Intelligence Council, "Disruptive Civil Technologies: Six Technologies With Potential Impacts on U.S. Interests Out to 2025," April 2008.

[3] ZDNet. "Is the Internet of Things strategic to the enterprise?" May 31, 2014. Available at http://www.zdnet.com/is-the-internet-of-things-strategic-to-the-enterprise-7000030068/

This risk, coupled with the asymmetric nature of the cybersecurity threat, requires an immediate and coordinated response from the public and private sector in order to ensure that the benefits of IoT are realized and the dangers are minimized. In order to understand this risk and develop recommendations to address it, the NSTAC engaged with key stakeholders from the Federal Government and industry subject matter experts, including organizations helping to lead and shape the future of the IoT. This allowed the NSTAC to garner insights and best practices related to the rapidly evolving IoT technologies.

The NSTAC found that IoT technologies are creating unprecedented effects. It is expected to boost the economy and improve life for citizens, particularly when combined with other related technology concepts, such as cloud computing, autonomy, and big data. There are also factors that could prevent IoT from reaching its maximum potential benefits, including failure to manage the risk associated with rapid innovation and increased connectivity, the lack of an institutional support structure for the IoT, and the inability of governance and policy processes to keep pace with the rate of development and deployment of emerging IoT technology.

The NSTAC also found that the compromise or malfunction of IoT devices could have NS/EP implications. Compromise of devices that run or are connected to different critical infrastructure systems could have the potential for major economic disruption, kinetic damage impacting public safety, or in extreme cases, catastrophic failure of national infrastructure or critical systems. Yet, it remains an open question whether IoT is being adopted in a manner that maximizes its utility and minimizes any associated risk.

Recommendations

In light of the rapid adoption of emerging technologies and the dynamic threat environment, immediate action is needed to address the dynamic IoT environment. The NSTAC found that existing governance, policy, and institutional support structures are not well-equipped to facilitate the rapid changes needed; therefore, NSTAC suggests the first three recommendations be acted upon within 90 days. Based on the authorities and responsibilities established by EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, the NSTAC recommends that the President execute the following recommendations:

1. Direct the Department of Commerce, specifically NIST, to develop a definition of IoT for use by departments and agencies to be used during assessments related to the IoT.

2. Direct the Office of Management and Budget to require Federal departments and agencies to:

    a. Conduct an internal assessment to document IoT capabilities that currently support and/or planned for support of NS/EP functions. These assessments must consider interconnections and interdependencies that may be introduced and the associated risks and benefits with respect to NS/EP.

    b. Develop contingency plans to identify and manage security issues created by current and future IoT deployments within the Government. The plans should recognize that IoT devices and their potential uses will continually evolve as well

as anticipate an environment that cannot be fully secured because of the dynamic nature of the IoT and the potential threat.

3. Create an IoT interagency task force that coordinates with existing organizational bodies to foster balanced perspectives between security, economic benefits, and potential risks. At a minimum, participants should include the Department of Commerce, Department of Homeland Security, and Department of Defense. The task force will set milestones for completion of the following activities that are reflective of the urgency of need to address the risks that ongoing deployments of IoT pose to NS/EP.

    a. Identify the gaps between security practices and emerging technologies to address the unique risks posed by IoT on NS/EP and develop plans for how to incentivize development of security innovations to address the gaps.

    b. Direct the update of Federal strategic documents to consider the security aspects of the explosive growth of and reliance upon IoT devices. Examples include the National Strategy to Secure Cyberspace, the Comprehensive National Cybersecurity Initiative, and Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program.

    c. Direct the update of existing awareness and training programs. The focus of the awareness should be to inform the public, as well as leaders and decision makers (private and public, including legislators), about both the benefits and risks of the rapid adoption of IoT and, thereby, encourage a culture of security around IoT device use and development. Role-specific programs should be considered for those involved in the design, development, production, procurement, and operation of NS/EP systems.

    d. Encourage and incentivize academia to develop curricula focused on: (i) IoT and the associated security challenges; and (ii) the convergence of the IT and OT disciplines, in order to educate future professionals engaged in the design, administration, or security of NS/EP systems.

    e. Encourage engagement in appropriate international forums for standards and policy development.

4. Convene and facilitate a Government and industry standing body to coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks. These guidelines should include the integration of IoT into systems that support NS/EP functions and highlight the gaps between risks the market will address and national security risks, which markets are not intended to address and are for use as part of the acquisition, procurement, and operations procedures. The result should enable an adaptive set of guidelines, focused on cybersecurity and resiliency of the ecosystem, that changes with the risk in a timely manner based on a continuous collaborative process. The executive agent of this standing body must have authority and oversight to enforce agreed-to deployment guidelines across governmental agencies and departments.

5. Direct the NS/EP Communications Executive Committee to: (1) review and recommend updates through the PPD-1 process on priority schema to account for and enable priority on all forms of next generation networks communications (e.g., voice, video, data) for NS/EP and public safety communications; (2) appropriately account for the impact the growth of IoT and IoT-related data associated with NS/EP communications; and (3) develop, in conjunction with the private sector, updates to NS/EP programs including Government Emergency Telecommunications Service, Wireless Priority Service, Telecommunications Service Priority, and Special Routing Access Services..

6. Direct the Office of Science and Technology Policy to review current research and development (R&D) investment and recommend future R&D funding for IoT security. Funding will help to understand the potential risks to NS/EP functions associated with IoT in an interconnected ecosystem, including IoT architectures, network management, privacy, and device identification and authentication in a manner that allows for productivity, growth, and innovation. Measure improvements in adoption and implementation of new technologies from the research execution with linkages to national priorities and interests and ensure that existing, similar recommendations are appropriately executed.

As recommendations are considered and implemented, it will be important to: (1) establish metrics to measure and monitor the effectiveness of the recommendations; (2) incorporate IoT technology in a manner that minimizes risk; (3) incorporate IoT in current education and awareness programs; and (4) ensure IoT-related R&D projects are addressing evolving cybersecurity challenges. The NSTAC believes these actions will help maximize security and resiliency within the IoT ecosystem.

1.0 INTRODUCTION

In 2008, the U.S. National Intelligence Council warned that the Internet of Things (IoT) would be a disruptive technology by 2025.[4] The Council said that individuals, businesses, and governments were unprepared for a possible future when network interfaces reside in everyday things. Almost six years later, this warning remains valid, though it now seems certain that the IoT will be disruptive far sooner than 2025—if it is not so already. More recently in January 2014, the Director of National Intelligence (DNI) stated that "[t]he complexity and nature of these systems means that security and safety assurance are not guaranteed and that threat actors can easily cause security and/or safety problems in these systems."[5] Several statistics validate the Government's concerns: the number of Internet-connected devices first outnumbered the human population in 2008, and that number continues to grow faster than the human population. By 2013, there were as many as 13 billion Internet-connected devices, and projections indicate that this will grow to 50 billion or more by 2020, generating global revenues of greater than $8 trillion by 2020. Many of these systems are visible to any user, including malicious actors, as search engines are already crawling the Internet indexing and identifying connected devices.

The IoT is the latest development in the decades-old revolution in communications, networking, processing power, miniaturization, and application innovation and has radically altered communications, networks, and sensors. The IoT is a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world. However, the IoT differs from previous technological advances because it has surpassed the confines of computer networks and is connecting directly to the physical world. Just as modern communications have fundamentally altered national security and emergency preparedness (NS/EP), the IoT has had a similar transformative impact.

Throughout the communications revolution, a plethora of existing and new technologies have led to astonishing improvements in the efficiency and effectiveness of Government and private sector operations and capabilities; yet the IoT differs in the pace, scale, and breadth of deployment of interconnected devices, which has resulted in immense benefits to individuals and organizations. Despite the benefits, the IoT is accompanied by risk associated with increased dependencies, expanded number of devices, and associated interconnections that will create a large attack surface with numerous potential threat vectors. The increased attack surface and our Nation's dependence on these new systems, either directly or through the critical infrastructure systems in which they are embedded, has made the IoT and new systems natural targets for criminals, terrorists, and nation states that wish to exploit them. These dependencies will continue to increase as the IoT permeates all sectors of the economy and all aspects of people's lives. While all users have to cope with this expanded attack surface, IoT applications in the NS/EP domain must be hardened against the potential risks. As IoT manufacturers and vendors

[4] National Intelligence Council, Disruptive Civil Technologies, Six Technologies With Potential Impacts on US Interests Out to 2025, April 2008.

[5] Clapper, James R., Statement to the Senate Select Committee on Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Committee, January 29, 2014. Available: http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

work to meet their customers' needs, including NS/EP demands, competition will ultimately determine which products and services succeed or fail, thereby fueling further innovation.

1.1 Scoping and Charge

Recognizing the IoT's pace of growth, breadth of usage, and depth of deployment, the Executive Office of the President, specifically the National Security Council, requested that the President's National Security Telecommunications Advisory Committee (NSTAC) conduct a study of the cybersecurity implications of the IoT within the context of NS/EP. In October 2013, the NSTAC's Designated Federal Officer established the Industrial Internet Scoping Subcommittee to examine the issue and present it to the NSTAC for consideration. Following member approval, a research subcommittee was established in March 2014. This report examines the implications of the explosive growth of the IoT in the NS/EP realm and will focus on potential changes to the security posture and associated strategies for NS/EP-sensitive infrastructures. These considerations will include the enormous expansion and morphing of the potential network-attack surface, the implications of the data explosion triggered by IoT, and the need to develop new disciplines focused on IoT and the intersection of information technology (IT) and operations technology (OT).

1.2 Approach

The NSTAC's approach was guided by the extent to which emerging IoT technologies are being deployed across a spectrum of users, from personal to national systems. In order to capture critical concepts, best practices, and lessons learned related to IoT technology implementations, the NSTAC engaged Federal Government organizations, as well as subject matter experts from industry. The engagements with industry included several industry-leading organizations that are working to help shape the future on how industry will best leverage IoT. Additionally, in the *NSTAC Industrial Internet Scoping Report,* four areas of the IoT were identified to help shape the NSTAC's research effort: (1) security; (2) operations; (3) design; and (4) policy. Each focus area of the IoT was used to inform the report's findings and recommendations and is described in detail in Appendix E.

Areas of Study in IoT

1) Security (Trustworthiness, resiliency, user behaviors, public/private partnership)
2) Operations (Interoperability of systems, reliability of operations, spectrum prioritization, IT/OT process coordination)
3) Design (Best practices and standards, security-by-design, trust relationships, integration with NS/EP programs)
4) Policy (Resiliency, privacy, public safety, international considerations)

The NSTAC also developed a strengths, weaknesses, opportunities, and threats (SWOT) analysis, depicted in Table 1, *IoT NS/EP SWOT Analysis*, which highlighted the IoT's benefits and significant NS/EP risks. This analysis helped the NSTAC prioritize its recommendations.

Table 1: IoT NS/EP SWOT Analysis[6]		
	Helpful	***Harmful***
Inherent to IoT	**STRENGTHS** • Ubiquitous sensing • Increased productivity • Speed and accuracy of information • Ability to immediately affect targeted change in the physical world	**WEAKNESSES** • Expanded attack surface (e.g., sensors, data) • Lack of clear technical public policy (i.e. identity management for IoT devices and users.) • Potential introduction of uncertainty due to high volumes of data • Data spread across multiple jurisdictions
Implications for NS/EP	**OPPORTUNITIES** • Real-time NS/EP operational efficiency • Expanded situational awareness with interoperable systems • Economic revenue growth • New functionality • Rethink end-to-end system security and resiliency	**THREATS** • Unanticipated attack modalities on NS/EP • Emergent, disruptive behavior • Immature knowledge base related to IoT security. • IoT traffic not currently included in NS/EP (Priority Telecommunications Services)

2.0 DISCUSSION

2.1 IoT Overview

Systems underpin every facet of American society—from transportation to utilities to communications—and are accessible and often controllable from around the world. More devices are connected to networks, and those networks are connected to each other, a concept known as the IoT; however, there is no universal definition of the IoT, just as there is no agreement in the use of that name to describe this trend. Whether it is called IoT, the Industrial Internet, or cyber-physical systems (CPS), the term describes a decentralized network of objects (or devices), applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical environment. These devices range from small sensors on consumer devices to sophisticated computers in industrial control systems (ICS). Ultimately, the devices have some type of kinetic impact on the physical world, whether directly or through a mechanical device to which they are connected.

IoT devices generally share three common properties:

1. Ordinary objects are instrumented, meaning that objects within a network can be addressed individually;
2. These physical objects are interconnected; and
3. The devices are intelligent and many can perform functions adaptively, either on their own or in collaboration with other devices and/or applications, based on their programing or a combination of that programming and the inputs collected from the physical world.

[6] This SWOT analysis was constructed to aid the IoTS in its research and development of the report. It is not intended to capture all of the strengths, weaknesses, opportunities, or threats of the IoT, but should serve as a representation of some IoT related topics of national importance.

Many types of devices, in infrastructure sectors across Government, industry, and private life, are rapidly being designed with functionality to sense some physical phenomenon (e.g., motion or specified levels of heat or light). When prescribed conditions are met, these adaptive devices perform the designed function without further command or authorization from a human being or another computer. Such devices can also receive remote commands to perform a function (e.g., open or close a switch or valve or operate machinery) using the communications connectivity inherent in IoT design.

While the term IoT is relatively new, the underlying concept of connecting computers to machinery is not; factories and large industrial machines have long been controlled by computerized ICS, and supervisory control and data acquisition (SCADA) systems that monitor and adjust industrial machinery based on operating conditions. Networking devices and connecting those networks to broader networks is also not revolutionary; however what sets the IoT apart from historical IT advancements is its explosive proliferation in three dimensions:

- First, the scale of deployment eclipses anything ever seen before in terms of pace of adoption. Estimates vary, but it is widely accepted that just five years from now there will 26 billion to 50 billion IoT devices deployed. By comparison, more than a generation after mobile phones became widely available, approximately only six billion are in use;
- Second, the scope of deployment ranges from the most complex system to the simplest device, from major manufacturing facilities and control centers to consumers; and
- Third, the demographic span of these deployments is spreading rapidly, leaving no aspect of infrastructure untouched by this phenomenon.

Because the IoT will touch all facets of American society, it will create new—possibly unknown—connected networks and interdependencies. Water, power, emergency services, healthcare, agriculture, and transportation are increasingly dependent on IoT devices. This creates a circular dependence among the devices, as IoT devices themselves are dependent on an array of other IoT devices that facilitate the delivery of essential services, such as power, communications, and data.

The IoT will influence and affect NS/EP regardless of whether or not consumer-oriented platforms have a direct connection to NS/EP systems. All workers in both Federal and commercial NS/EP-related organizations and infrastructures will be impacted by the bombardment of IoT into consumers' daily lives. The effect is inescapable, and no amount of effort will suffice to prevent it, even if that were attempted in the name of security. In the *NSTAC Report to the President on Secure Government Communications*, the NSTAC examined how modern IT, as embraced by workers and used in NS/EP-related workflows, alters the security profile of unclassified Government work. The report's findings, conclusions and recommendations are validated by the new IoT phenomenon.[7] Rapid IoT deployment underlines the urgency of increasing awareness of the risks and benefits of new technologies that are now in broad use and that require innovative approaches to security. At the same time, the installed base of what might be termed the "industrial" IoT will be penetrated in new ways, with historically

[7] National Security Telecommunications Advisory Committee. *NSTAC Report to the President on Secure Government Communications*, August 20, 2012. Available: https://www.dhs.gov/publication/2013-nstac-publications.

isolated OT becoming accessed and influenced by both authorized users and malicious actors. Taken together, the IoT's broad proliferation into the consumer domain and its penetration into traditionally separate industrial environments will progress in parallel and become inseparable.

The rapid adoption of IoT enables many immediate and tangible benefits. Connected machinery can run more efficiently and is more reliable because it can self-report potential failure indicators before they occur. Connected healthcare devices can improve patient outcomes. Advanced logistics can simultaneously enhance a retailer's ability to deliver commercial goods and the Federal Emergency Management Agency's ability to manage a disaster response. Citizens also see direct benefits and use of IoT devices to simplify and improve their daily lives.

The IoT poses risks as well. For an individual consumer, the risk is often minor; the failure of commercial IoT devices may be inconvenient, but generally do not threaten life or national security. Medical devices, however, including implantable ones, differ because an increasing number of them have built-in connectivity. It is possible that a compromised or malfunctioning IoT healthcare device could lead to patient deaths. The DNI recognized this in his January 2014 statement before Congress, noting that due to "the cross-networking of personal data devices, medical devices, and hospital networks, cyber vulnerabilities might play unanticipated roles in patient outcomes."[8] The IoT also increases risk to personal privacy, as most IoT devices collect, analyze, and store data.

There are also national implications that could arise from the compromise or malfunction of IoT devices that run—or are connected to—different critical infrastructure systems. Critical infrastructure IoT devices are increasingly automated and adaptive, collecting data from the systems they control and then acting on that data; failure of some of these systems would have profound national impact. These impacts could be economic (e.g., lost productivity and damage to the national economy) or in the public safety realm (e.g., kinetic damage or in extreme cases potentially catastrophic failure of machinery or infrastructure).

Though perhaps foreseen by some technologists, the explosion of the IoT and the ever-increasing connectivity of such a wide range of systems were not factored into the design of many of the current network systems and machinery. As a result, there may be cybersecurity risks associated with the traditionally poor connectivity of the OT and IT domains, the intersection of which is sometimes referred to as a collision or convergence.

IT and OT have historically responded to very different demands and have very different baseline planning assumptions in everything from risk tolerance to the development process. For example, IT devices and software have lifespans of months or sometimes years, while the OT refresh cycle is often measured in decades. Historically, IT and OT are largely viewed as separate disciplines in the research and development community and in academia. To minimize potential risks created by the IoT, this gap must be addressed in a way that includes security and resilience considerations from the outset.

[8] Clapper, James R., Statement to the Senate Select Committee on Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Committee, January 29, 2014. Available: http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

The IoT has also begun breaking down barriers between commercial and industrial technology, as devices and software that were intended to be consumer-focused are increasingly being used in the manufacturing and national security domains. Moreover, it is likely that some low-power, inexpensive devices and technologies, including software applications, that gain wide acceptance in consumer or highly-commoditized IoT applications will either be connected to infrastructure systems or will be used as building blocks of more complex mission critical products. As a result, security decisions that are made, and security flaws that are introduced, in the context of a consumer device may have more far-reaching implications than with previous innovations.

2.2 Considerations of the IoT Impact on NS/EP

Based on the pace of deployment of IoT technologies, the IoT will potentially impact NS/EP, from how critical services are delivered to citizens to how the Nation is protected. Widespread use of IoT devices allows expanded situational awareness and data and analysis that will enhance critical infrastructure operations, as is evident in such initiatives as Smart Cities, Smart Grid, and Smart Transportation, as well as in the myriad of smart consumer devices that are being introduced to individuals, larger enterprises, and corporate networks. The speed of innovation and deployment does not appear to be slowing.

The open and integrated IoT environment is expected to boost the economy and improve life for citizens. When combined with other related technology concepts (e.g., big data, cloud computing, robotics, and autonomy), the IoT is expected to produce unprecedented effects for users at all levels. Other factors may prevent the IoT from reaching its maximum potential, including failure to manage risks associated with rapid innovation and increased connectivity, the lack of an institutional support structure, and the inability of governance and policy processes to keep pace with the development and deployment of emerging IoT technology.

2.2.1 Unique Aspects of IoT Technology

The IoT may be the most disruptive phase of the Internet revolution. Physical objects, data stored remotely, and the natural environments will all interact with one another. Despite consensus on the great potential provided by IoT technologies, there appears to be a general lack of vision and objectives on how to best maximize the potential benefits of IoT relative to NS/EP while ensuring appropriate risk management. Additionally, current governance processes do not appear well suited for, or aligned with, the pace of change associated with IoT innovation. The number of IoT devices being deployed continually rises, which exposes—or creates—gaps related to standardization, interoperability, and identity validations as modularization of IoT technologies are deployed.

2.2.1.1 Proliferation of IoT Devices

The gaps created by the IoT increase the potential that some devices may be invisible or not detected by the networks to which they are connected, thereby making it difficult to protect them from threat actors. It is therefore axiomatic that the attack surface for bad actors has increased exponentially. Additionally, many consumer and industrial devices rely on embedded processors that were originally installed without any intent to connect them to a network; however, now, building heating, ventilating, and air conditioning controls, manufacturing plant systems, and

automotive breaking and steering systems can have interfaces that enable remote monitoring and system control. As the use of IoT devices becomes more pervasive, it will be difficult for organizations to avoid becoming dependent on the functions provided by IoT sources and products. Just as mobile communications have shifted communications dependency from land line communications and rendered the payphone obsolete, smart devices will become impossible to avoid. As these devices proliferate, it is important to ensure that they are deployed in a security-informed manner and in ways that minimize future risk. Clear guidelines are needed to aid organizations in making security-informed decisions before connecting legacy systems or embracing new IoT technology.

> Massive increase in the volume of data offers new opportunities for real-time NS/EP operational efficiencies, as well as improvements for quality and safety of life; yet, the benefit comes with tremendous cybersecurity risks, including data veracity and privacy.

A White House Presidential Innovation Fellow project, called the Smart America project showcased how entire cities and economic sectors (e.g., transportation and energy) incorporate the benefits of the emerging IoT technologies.[9] The project demonstrated the great promise of IoT, yet also highlighted two key observations: (1) the engineering and design culture of the IoT places functionality and speed to market above any security concerns; and (2) there is currently no accepted repository, clearing house process, or organization to capture lessons learned so that they can be easily be built upon by others.

2.2.1.2 Exhaustive Volumes of Data

The deployment of billions of interconnected smart devices is producing increasingly voluminous amounts of data that can be used in a number of ways. An unintended consequence of the new sources of data is the generation of "data exhaust," that, when examined by threat actors, could reveal significant insights (e.g., geolocation or biometrics of national leaders). The potential uses of the data collected by IoT devices are endless.

Until recently, the data collection was conducted in silos and data tended to remain in its original unit or organization. IoT and its near-ubiquitous interconnectivity changes this; data aggregation and the broad use of data by disparate individuals or organizations are now standard. Data aggregation services for enterprises and consumers will prove invaluable in sifting through the volumes of new data generated by IoT devices, but they will also become new focal points for attacks and privacy violations. This can provide great societal benefits through process optimization, resource allocation, and decision making. Early benefits of optimization are already being realized within selected sectors of critical infrastructure, including health, energy, and transportation. The data explosion, often called big data, is not new, but will impact every sector as data analysis underpins new waves of productivity, growth, and innovation. Nevertheless, capturing the full potential of big data is a challenge. Moreover, billions of devices creating, transmitting, and storing data will create data exhaust, which can create vulnerabilities that are not readily apparent; often the data may include sensitive information, such as, telemetry, voice, video, health, and infrastructure component status data. Privacy, security, intellectual property, and use policies will need to be updated to reflect this new reality.

[9] Smart America. Available: http://smartamerica.org/

More experts are needed who can take full advantage of the data made available by IoT, and organizations may be challenged to optimize the use of big data. This includes an understanding of the controls in place to protect the data and systems that transmit, process, and store the data. Access to data is increasingly critical as organizations and agencies attempt to integrate information from multiple data sources.

2.2.1.3 Blurred Roles & Functions of IT and OT Networks

The IoT blurs the boundary of IT and OT. Over many years, IT and OT have developed their own constituencies, values and equities, roles and missions, and user cultures. Most importantly, IT and OT have developed very different approaches to security: IT security revolves around patches and frequent updates (and the ability to take systems offline, as needed), and OT security revolves around obscurity and specialization (and the need for systems to remain online, whether compromised or not). Within the IoT, these domains interact dynamically.

As recognition of the blurring of IT and OT spreads across the design and user communities, IT and OT practitioners have sought to convince their counterparts of the need to accommodate their equities, cultures, and usages, for reasons grounded in their own concerns and experiences. There is little evidence of any broad progress in these efforts in favor of either viewpoint or movement towards a consensus that balances them. As the IoT—whether characterized as primarily oriented towards IT or OT—continues to proliferate along the explosive trend lines, a new paradigm is needed in which IT and OT are considered as an integrated, single concept. Over time, where IT and OT systems interact within the IoT, they increasingly assume some of the qualities of each other, and become less clearly definable as "pure IT" or "pure OT." Technology will lead, and technology operators tend to expand the boundaries of how devices are used.

In order to understand the relation to the IoT, it is important to recognize the similarities and differences in how a device can be used, as opposed to whether a device is considered IT or OT. There are many cases in which a single technology or system can be used for many different purposes. For example, a modern desktop computer can be dedicated to support a manufacturing function and, as long as it does so in isolation from the larger IT environment, it can do so safely and efficiently for an extended period of time; however, if and when that machine is connected to Internet-based processes, the operators of that machine must recognize the need to embrace security principles and practices normally associated with IT. From a cybersecurity standpoint, this connection to the Internet causes dedicated manufacturing-support machinery to become vulnerable to the same attacks and exploits.

In the case of IoT devices, there is a strong trend toward purposeful design and fielding machines that are intended to straddle classic IT and OT functionality so that clearly delineating a machine as IT or OT becomes pointless or impossible. Rather than classifying these devices according to existing norms that do not fully capture their capabilities, this technology may become recognized as a discipline of its own—a sort of hybrid technology.

Recognizing the hybrid nature of today's devices offers a number of insights and advantages. At the level of basic enabling technology and design, where commonality is at its greatest, it may be possible to define and describe standards and other design elements most beneficial to security.

This can include engaging an IT-based standard security package, network port security, or intrusion detection on the local network. Doing so through a hybrid security approach offers the best chance of achieving broad benefit across the IoT domain. The intent of hybrid security efforts may be to identify and treat security issues common to all IoT devices, regardless of deployed domain or end user, which would allow end users and application managers to focus on threats and needs specific to their own domains. Many devices and systems will be employed in hybrid operational settings for their entire lifespan. In fact, IoT will likely grow and demographically expand more rapidly than pure-IT or pure-OT domains, which are already well developed in many areas. For these IoT devices, common security practices will offer the maximum benefit.

At the end user and deployed system level, many devices are employed in specific applications and operational settings unique to either manufacturing or IT-network operations. These are more specialized and optimized for the needs and requirements of their owner and operators. Security and other management decisions and responsibilities for these domain-specific devices are not altered by recognition of the emergence of a hybrid technology, except that, over time, managers may hope that new IoT technology will have benefitted from core security attention before they receive it. For purposes of NS/EP, hybrid security standards and practices can be deployed and tailored in defined NS/EP areas of interest and responsibility. For example, an IoT device used in disaster response will have different utility and security needs than when it is used in a combat zone. Security should be appropriate to both the device and to the specific use case.

In operational environments, end user organizations will often be the last to adapt to the new technology, as the full effect of the technology is realized, recognized, and assessed. In this case, the emergent need is for an organizational focus of hybrid processes. Since the technologies are fully OT and fully IT, but not exclusive to either, it is be important to create a management environment and processes that will import all needed considerations and cultures of both industrial and network operations into development and management of security standards and practices for common-core hybrid technology.

2.2.1.4 Security in the Evolving IoT Ecosystem

As previously noted, the IoT will have a broad impact on NS/EP. The scale of deployment and the extent of interconnectivity could lead to events that occur very quickly and cascade before a response is possible. Each element of the ecosystem introduces additional security risks and IoT devices are being deployed at a rate that is faster than these risks can be understood. In such environments, cybersecurity processes that emphasize centralize control or that focus on individual systems are insufficient to address the security and resiliency of the IoT. The IoT creates opportunities for new thinking on approaches to end-to-end ecosystem security and resiliency, where decisions can be made automatically in a distributed manner and use an agreed-to set of principles that enable near real-time responses to NS/EP events.

Trustworthiness

Trustworthiness involves the overall IoT ecosystem, from devices and systems to data and algorithms. It also includes the need to consistently and reliably perform to a level of security. Trustworthiness will vary with the device and use, but NS/EP applications require the highest level of assurance. In a distributed environment, this may be achieved by having best existing

security practices and principles internalized, practiced, and implemented by each IoT developer, programmer, or installer. It may mean pushing security processes down to every potential element of the ecosystem as they are developed and deployed; defense-in-depth will often be a reasonable course of action to embrace.[10] The principle of "don't trust and always verify" (i.e., systems should not trust the data that is received and always verify any interconnections) should be integrated into the design of IoT ecosystems, and will be particularly important in NS/EP applications.

Stakeholders should consider the following practices to enhance IoT security by adapting existing security-by-design best practices and cybersecurity:

- **Minimizing known vulnerabilities and reducing the security risks posed by new IoT devices:** IoT devices vary greatly in capabilities, ranging from simple sensors to sophisticated systems, with corresponding variation in potential risks. Device classifications and best practices in the design, development, and manufacturing of these different classes help to minimize known vulnerabilities during their entire lifecycle, including the production cycle. As much as possible, devices should be designed to be future compatible, incorporating mechanisms that would facilitate inevitable future upgrades of any ecosystems of which they may become part. These mechanisms may vary for different classes of IoT devices and devices used for NS/EP critical functions requiring highest levels of security. Capable devices may send periodic notifications of upgrades or be able to learn new algorithms to improve their operations over time.
- **Identifying and assessing security vulnerabilities of existing IT/OT/IoT deployments and develop appropriate threat models for NS/EP:** The full scope and potential risks of the IoT/IT/OT networks on NS/EP should be mapped and tested, including interdependencies and human interfaces. The increased use of unsecured personal devices over public networks to connect with public infrastructures creates heightened risks, and the ubiquity of IoT devices exacerbates the need for analysis.
- **Developing a data taxonomy with potential NS/EP impact for additional security protection:** The majority of IoT devices operate via the Internet or on other unprotected networks, many of which have limited storage and processing capabilities. As a result, data is transmitted to a central location for further processing, which increases the opportunities to compromise the data and exacerbates the potential impact of any data breach. Stakeholders should develop an appropriate data taxonomy to identify IoT data with NS/EP impact for varying levels of protection.
- **Creating IoT systems with transparent behaviors and functions:** IoT devices and systems deployed that may have NS/EP implications should have well-understood and well-documented or observable features, functions, and interdependencies.
- **Developing interoperable security and trust frameworks to enable threat information sharing:** The IoT can provide unprecedented detailed information to predict and counter attacks. For example, information from multiple types of sensors can provide data for

[10] According to NIST Glossary of Information Security Terms, NISTIR 7298 Revision 2, defense-in-depth is an information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.

advanced, automated threat diagnostics. This will require interoperable security and trust frameworks to enable collaboration, especially between jurisdictions.

- **Exploring new NS/EP security models, especially at the ecosystem level, where security decisions can be made autonomously and at speed and scale:** The dynamism of the IoT introduces new adaptability requirements to existing security practices. For example, as part of security-by-design, it is necessary for components and systems to be able to learn and detect new vulnerabilities dynamically, and if necessary, isolate themselves. Furthermore, it is no longer sufficient to examine security at the individual component or system level. It is critical to explore techniques to detect and enable end-to-end security at the data-ecosystem level due to the IoT interconnectedness. Finally, the varying capabilities of IoT devices may require that they cooperate with one another to provide the appropriate security levels for an entire system.

Resiliency

Government and industry must manage risks to IoT systems supporting NS/EP functions. The security of IoT remains particularly hard to influence because of its nascent state, the rapid trajectory of deployment, and the breadth and diversity of devices; the number of actual and potential vendors of IoT devices; and the lack of technical standards and operating procedures. As such, it is unlikely the security of the IoT can be fixed in the near-term before deployment; therefore, Government should develop contingency plans to address IoT deployments in Federal departments and agencies. Comprehensive planning for unsecure environments should consider technical concepts such as upgradeability, as mentioned above, but also other technical, architectural (e.g., control plane and management plane separation), and policy and planning efforts (e.g., updates to continuity of operations/continuity of government), should be updated to promote resiliency.

In the early stages of an event, it may be difficult to determine if a cyber attack or reliability failure is occurring. The IoT requires a paradigm shift from protect-detect-respond to one that emphasizes survivability of the ecosystem and minimizes the negative impacts on physical systems. The ecosystem's resiliency will be particularly important for IoT systems with potential NS/EP implications—no single or set of attacks should cause a catastrophic failure of the ecosystem. The ecosystem must remain operational even with some number of compromised systems.

To do this, IoT systems should leverage current strategies used in online services. For example, system developers and administrators could deploy a measurement and reporting methodology that collects and analyzes a base set of key performance indicators unique to a given IoT network. Such a process is critical to leverage the extended surface of the IoT, as it will help mitigate a system's potential cascading failure effects, which can consist of many adaptive autonomous parts and where human interaction may not be involved.

Sharing information across the ecosystem about IoT-related events will be essential. An interconnected environment where systems independently make decisions presents structural problems that pose risks to the greater networks. Processes such as information sharing should be in place and pre-coordinated to immediately localize any damage.

Individuals

Individual behaviors are critical in any security framework; however, this is exacerbated by the combination of IoT devices and NS/EP considerations. This criticality arises from two unique IoT challenges: (1) the interconnectedness of the ecosystems; and (2) the increased surface of attacks. As a result, any device can be a potential source of entry into the ecosystem and an opportunity for increased situational awareness. In such widely distributed systems, individual awareness of threats and risk and the use of secure devices are an essential element of the risk mitigation processes. Consumer demands can also drive the market to demand IoT devices and services with higher security standards.

Partnership with Industry

With the tremendous economic opportunities offered by the IoT, industry has taken the lead in developing IoT innovations in a wide variety of sectors, including manufacturing, energy, transportation, communications, retail, healthcare, and urban development. As companies recognize the need to develop interoperable platforms and systems, multiple industry consortia (e.g., Open Internet Connection Consortium and the Industrial Internet Consortium) have formed to address different parts of the ecosystem and different sectors. The Government needs to leverage this innovation and best practices in partnership with the private sector to address the IoT impacts on NS/EP.

2.2.1.5 Automated and Adaptive Behaviors of IoT Systems

IoT systems are end-to-end and consist not only of the physical connections of sensors and devices to a network, but also the software, systems, and algorithms that are used to analyze the data collected by these objects. These systems also include any adaptive behaviors exhibited by the objects, either through pre-programmed or machine learning algorithms. Although these are automated behaviors, the fact that their functions can be reconfigured based on machine learning algorithms introduces a certain level of unpredictability. Various IoT literature describes these systems as autonomous systems. This aspect of the IoT introduces an additional factor affecting NS/EP in that systems may be re-programmed to change their behaviors automatically through specific inputs of data or interaction with other systems. This can be positive (e.g., quicker response to a threat or a situation) or it can be negative (e.g., cascading effects that may be difficult to control). In the worst case scenario, such systems can either cause or exacerbate NS/EP events faster than humans can participate in or react to them.

2.2.2 IoT Governance Considerations

Appropriate governance, particularly when developed through a public-private partnership, is essential to ensuring large scale system interoperability and integration. The recent National Institute of Standards (NIST) Cybersecurity Framework and the *Report of the Commission on Cybersecurity for the 44th Presidency* are examples of this type of partnership.[11] The IoT will require the same governance and public-private partnership cooperation, but the need is

[11] Center for Strategic and International Studies. Securing Cyberspace for the 44th Presidency. Available: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

particularly acute because of the combination of the rapid adoption of IoT devices and the significant NS/EP implications of this phenomenon. IoT requires the development of governance and policy structures much more quickly than the norm. Moreover, because the IoT is global and borderless, good governance will require international engagement.

2.2.2.1 Policy Review Cycles

Technology typically advances faster than policy, leaving a gap between technological reality and policy development; however, because the IoT is advancing quicker than previous technological developments, this traditional gap is turning into a chasm. For example, privacy concerns are raised by increased data collection and uses associated with new technology deployments without appropriate established guidelines regarding security and privacy.

As noted, IoT adoption is forecasted to reach 50 billion machines and devices or more in the coming years. This is analogous to the state of cellular mobile services in 1994, a time when cell phones were in wide usage, yet it was still impossible to anticipate the future changes; while similar, IoT usage will grow significantly faster than cell phone usage. Government is still working to develop policy to address the growth of mobile phone usage, and IoT policy already lags far behind. Importantly, many national level documents that provide strategic direction related to cybersecurity do not address—or even mention—the IoT. The Government must move quickly to address the threats and vulnerabilities this technology will bring to encourage responsible IoT innovation and enable continued economic growth.

With national policy lagging, the Government cannot rely on existing policy development mechanisms, but instead must seek new methods to leverage the private sector knowledge, particularly regarding emerging advance technologies, in the development of IoT policy. The Government can be most productive by convening experts to build consortia or other bodies that can provide guidance for Federal policy, as well as private security best-practices and governance. Additionally, existing consortia composed of specific communities of interest should consider cross-sector facilitation and top-level architectural guidance that takes into account enterprise-level and national security. The Government is uniquely positioned to facilitate such cross functional work. For the IoT, an effective approach may be to focus on case studies that provide best practices and success stories of how IoT is being addressed in different industries and then gauge the NS/EP implications.

2.2.2.2 Governance Structure

Effective security for the national cyber environment requires consensus-based standards, best practices, and guidance on their application in a variety of environments. These will need to be combined with collaborative mechanisms for trusted and valued information sharing to identify and respond to inevitable flaws as quickly as possible. It is essential that the Government develop an authoritative structure for codifying, evolving, and using informed expert judgment to apply known standards, practices and other criteria for cybersecurity. NIST is responsible for developing and applying Federal computer security standards and guidelines for civil departments and agencies and the National Security Agency is responsible for the national security departments, agencies, and systems; however, there is no analogous information systems security focal point for the private sector. In fact, the numerous companies and organizations

engaged in the cybersecurity realm that advise owners, operators, and users is confusing to many, overwhelming to small and medium entities, and largely invisible to most end users.

Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, released in February 2013, has served as one of the focal points for working with private and public entities to develop a cybersecurity framework.[12] The Framework, developed by NIST, provides broad guidance for applying risk management practices and existing cybersecurity and privacy standards to a range of operational environments. The Framework does not, however, provide detail and guidance for specific situations, leaving those decisions in the hands of the organizations that elect to use it. Some sector organizations have begun to fill that void based on their sector's needs, but these too will require each organization to secure its own unique systems.

These efforts are making steady, but slow, progress in what has become the realm of traditional cyberspace. However, today's cybersecurity environment shows that failure to consider security, safety, and privacy early in the adoption period makes late adoption harder and more expensive; it is far more affordable and there are more choices of devices for those considering and planning for inevitable attempts to exploit new systems or capabilities while still relatively nascent. A robust, private sector-led mechanism to encourage the production and adoption of cyber devices and systems can enhance the security, safety, and privacy of the Nation.

2.2.2.3 Privacy Considerations

Existing data privacy standards and concepts do not translate well into the IoT environment where data accessibility has expanded across multiple related communities of interest based on omnipresent network connectivity. The proliferation of data-generating devices has significant benefits but is also susceptible to malicious or other unanticipated uses.

A recent study from Hewlett-Packard found that more than 90 percent of all IoT devices examined collected at least one piece of personal information. Of these devices, 80 percent of these failed to use sufficient authentication. Additionally, 70 percent of tested devices used no encryption when transmitting this data, allowing data downloaded from the devices to be intercepted, viewed and modified.[13] The massive amount of data that sensors can aggregate about individuals has enormous value to marketing and businesses efforts, first responders, and medical and behavioral research.

Nevertheless, there are more malicious uses of data. When data is collected without knowledge or consent, people may not be aware of the types of conclusions businesses and Government can draw about their lives, habits, and inclinations; moreover, when aggregated on a large scale, seemingly innocuous data elements can be combined to facilitate identity theft on a scale not previously seen. Additionally, aggregated location-based data can allow individuals, including national leaders, to be tracked.

[12] EO 13636, *Improving Critical Infrastructure Cybersecurity*. February 19, 2013. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[13] Hewlett-Packard. *Internet of Things Research Study: 2014 Report*. Available: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

Privacy-by-design is one way to address these concerns. Privacy-by-design is privacy built in at project initiation, allowing data to be anonymized at collection and provides users with information regarding the collected data and the control they have over that collection. Data collected anonymously protects privacy while benefiting the aggregate analysis. First responders, traffic engineers, and other organizations can use the data to benefit society as a whole.

Privacy has an important linkage to NS/EP, and this topic is being addressed through other privacy studies and initiatives. NIST has begun a privacy engineering initiative that facilitates moving from process-oriented principles, such as those associated with the Fair Information Practice Principles (FIPPS) to risk management frameworks.[14] This is an excellent example of the Government and the private sector collaborating to develop governance norms.

2.2.2.4 Resiliency and Prioritization of NS/EP Communications

The growth of IoT will introduce unique capabilities and challenges to NS/EP communications in national security, emergency preparedness and critical infrastructure and key resources (CIKR) use cases. Existing NS/EP communications services, including Telecommunications Service Priority (TSP), Wireless Priority Service (WPS), Government Emergency Telecommunications Service, (GETS), and Special Routing Access Services (SRAS) will need to account for the IoT's unique properties. Some questions and considerations that the Government needs to address include:

Because IP-based data networks do not possess the same priority or dedicated connections functionality as traditional telephone networks, IoT devices cannot now leverage existing or planned NGN-PS features of GETS/SRAS PIN validation.

- If IoT devices are connected to wireline or wireless networks and are operating (e.g., sensor/actuator) in an NS/EP role or function, how can that device authenticate and receive network priority? Should it?
- TSP priority provisioning, restoration, and SRAS trunk allocation are physical, circuit-based platforms and technologies; as such, how should connectivity to IoT end-points be established, prioritized, and maintained?
- While data services have been contemplated in Next Generation Network Priority Services (NGN-PS), how will the unique properties of adaptive actuators/sensors operating in an NS/EP function be assessed?

In anticipation of rapid communications changes, the Government set forth authorities described in EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, states: "The responsibilities of the [NS/EP Communications] Executive Committee shall be to: (a) advise and make policy recommendations to the President, through the PPD–1 process, on enhancing the survivability, resilience, and future architecture of NS/EP communications, including what should constitute NS/EP communications requirements."[15]

[14] NIST. Privacy Engineering. Available at: http://csrc.nist.gov/projects/privacy_engineering/index.html

[15] EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*. July 7, 2012. Available: http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

The universal communications evolution that provides end-to-end voice, video, and data services over one Internet protocol (IP)-based network technology has created new opportunities as well as challenges for ensuring the functionality of existing NS/EP priority communications programs. As the communications industry continues to make technological advancements to reduce operational costs and provide increased bandwidth and network services, the Government must still fulfill its responsibilities, as outlined in EO 13618, for national leadership; Federal, State, local, tribal and territorial governments; and other authorized NS/EP users. The overarching goal of existing protective programs is to provide the ability to improve access and expedite restoration or provisioning for NS/EP communications services in the event of network congestion.

With respect to the NS/EP priority telecommunications services and their associated identity management architectures, IoT devices are unable at present to leverage existing or planned NGN-PS features of GETS/SRAS personal identification number validation, but could possibly use WPS subscription. To support IoT, the Government should review NS/EP policy to include consideration for non-human, end-point NGN-PS authorization, session establishment, authentication, and completion.

The Department of Homeland Security's Office of Emergency Communications (OEC) has established a contractual mechanism to support NGN-PS solutions to address challenges such as IoT. To further investigate how to incorporate IoT into priority services, the NS/EP Communications Executive Committee and OEC should expand NS/EP communications requirements to examine the impacts of IoT to include consideration of all aspects such as; non-human, end-point NGN-PS authorization, session establishment, and authentication.

In that regard, a major driver of IoT is the development of open, voluntary, and consensus-based standards. Ongoing and future standardization efforts that enable the success of the IoT will cut across market segments, and will range from overarching guidelines to specific technical criteria, ensuring increasing interoperability as well as backwards-compatibility. Importantly, these standards are able to dynamically adapt to needed changes based on the expertise across stakeholders. Numerous existing standardization efforts, as well as future efforts, to address industry-consensus needs will define and contribute to the development of an interoperable IoT. These standards efforts provide an opportunity for the Government to expand the growth of IoT in national security, emergency preparedness and CIKR use cases. Though not specific to NS/EP communications, standardization efforts such as Telecommunications Industry Association research standard TR-50 machine-to-machine (M2M) (Smart Device Communications) is an example of an area of interest. Another example is oneM2M, an international partnership working to develop technical specifications that address the need for a common M2M service layer that can be readily embedded within various hardware and software elements, among many others.[16]

Standardization is a form of economic self-regulation that can relieve the Government of the responsibility for developing detailed technical specifications while ensuring that voluntary, consensus standards serve the public interest, saving resources that can be used to serve the

[16] oneM2M. Available at: http://onem2m.org/

public in other ways. By taking this approach, Government policymakers can use standards as valuable sources of scientific and technical information developed with the assistance of private sector experts. Agencies can also use the standards as a resource for advanced technical information without first-hand independent knowledge of research in the area.

The IoT will rely significantly on maximizing the continuity of connectivity. Additionally, with the world rapidly becoming wireless, establishing an appropriate spectrum policy is essential to ensure that the IoT will be successful. Wireless connectivity is becoming the way in which consumers access the Internet from Long Term Evolution (LTE), Wi-Fi, and satellite technologies. Traditional Wi-Fi is also expected to play a key role in IoT deployment due to its low cost and ubiquity in the marketplace. Effective risk management will require a close examination of the network connectivity to ensure that its security and reliability is commensurate. When examining the risk taxonomy of IoT systems employed for NS/EP communications, it will be critical to ensure that appropriate network technologies are contemplated. Factors would include usage of licensed versus unlicensed wireless spectrum; prioritized (QoS) versus best effort connectivity; wireline versus wireless; and private line versus virtual private networks versus public networks.

The future IoT will likely be based on heterogeneous networks whereby devices can sequentially or simultaneously use different network technologies, wired or wireless. This opens the dialogue to examine how NS/EP IoT traffic will be measured across and through networks and may need to include some process guarantee for the completion of NS/EP IoT traffic.

2.2.3 IoT Institutional Support & Structure

The pace of IoT deployments and the associated impact on American society highlights the NS/EP implications and the need for institutional processes to capitalize on the potential benefits and minimize the risks associated with using IoT technology; however, such institutional processes are not fully established today. There is still a lack of a common definition and understanding of the term IoT and no coordinated efforts. As a result, IoT is not well understood and its impact not widely recognized. Education, training, and awareness in IoT are immature, and R&D is uncoordinated and without unified national priorities related to potential NS/EP uses. The development of IoT in the United States influences, and is influenced by, global R&D and standards.

2.2.3.1 IoT Education, Training, and Awareness in the Context of NS/EP

While IoT is a relatively new term, the associated education, training, and awareness related to CPS, ICS and SCADA systems are of particular interest in the context of NS/EP. The integration of ICS and IT systems is creating a shortage of trained professionals with combined OT and IT skills, therefore educational programs should also be updated.

The academic community is beginning to introduce IoT and CPS concepts into engineering, computer science, information sciences, data sciences, and cybersecurity-related courses, yet, programs are in the early stages. The concern is, as IoT continues to emerge and expand, the

complexity of operation is compounded as the retirement age work force is outpacing the rate of U.S. students majoring in the engineering fields.[17] People who understand complex systems in industry are retiring in large numbers at the same time that student enrollment in engineering degrees is declining.

Faculty at research universities and experts at research facilities in the U.S. are conducting research on some of the cybersecurity implications of this evolving technology, as is the NIST Cyber-Physical Systems Public Working Group. The National Initiative for Cyberspace Education (NICE) Workforce Framework can be leveraged to bring further national attention to IoT challenges and opportunities. NICE Component 1: National Cybersecurity Awareness Lead: DHS and Component 2: Formal Cybersecurity Education Co-Lead Department of Education and National Science Foundation are examples of programs already in place that could be updated to create more robust education and awareness programs to include IoT.[18]

Many cybersecurity experts in various sector-specific operations, including transportation and electricity, recognize the benefit of emerging IoT technologies and potential vulnerabilities to their critical infrastructure sectors; however, without access to an IoT awareness program, some may be more enamored with the new features and capabilities of the IoT technology and unaware of the risks. While awareness about the benefits and cyber risks of IoT needs to be raised at many levels, from private citizen to national legislators, it is particularly important for leaders and policy makers to understand the implications of using IoT technologies. Across Federal agencies, many IoT related efforts are underway, particularly those related to mobile network connectivity; however, they do not appear well coordinated to share the security implications related to IoT. Additionally, there is no central or combined repository (in either Government or industry) for collecting or sharing lessons learned regarding emerging technologies which could be useful for developing coordinated guidelines and awareness for NS/EP systems.

While deeply technical, IoT is also user-friendly. Government employees and the general public use IoT devices, often not knowing or caring about the details of the technology that underpins the device features and capabilities. The aforementioned contributes to the complexity of the challenges of IoT, as users are not likely to be aware of the risks associated with new capabilities until there is individual impact. New and innovative functions and features tend to motivate buyers; however, the more consumers are informed and aware of the IoT's risks, they will be able to help drive the market to adopt standards and guidelines that provide greater security, privacy, and resilience.

2.2.3.2 Research and Development

Unlike established architectures whose design and operations are well documented, the IoT is still evolving. Individual IoT technologies and systems exist, but there is currently no standard-based, large-scale IoT deployment in support of national security systems. Despite the consensus on the great potential of the IoT, and the significant progress in a number of enabling

[17] Tanya Lee Ann Crenshaw, "Using Robots and Contract Learning to Teach Cyber-Physical Systems to Undergraduates" 2012. IEEE

[18] National Initiative for Cybersecurity Education. Available at: http://csrc.nist.gov/nice/index.htm

technologies, the United States lacks an integrated vision on how to realize integrated, standard-based IoT systems.

IoT research at the system-level is still in its early stages. Most of the current research takes place in relatively narrow, discipline-specific venues in industry and academia. Research is typically partitioned into traditional disciplines, such as sensors, communications, operational technology, and energy efficiency. Workforce education and expertise is fractured in a similar way and presents a formidable challenge to the future design of IoT systems.

To enable a vision of ubiquitous, reliable, secure large-scale interconnected IoT systems and ensure a broad acceptance from individuals, organizations, municipalities and governments, coherent multidisciplinary research that aligns with the national strategy is required. Some of the key research areas are related to IoT architectures, including standards, identification, security, and privacy technologies and practices; and network management techniques.

IoT Architectures

Innovative approaches to architectures, interfaces, and abstractions that enable seamless integration of networks, sensors, control, and computation must be developed for rapid design and deployment of heterogeneous IoT systems. For example, in communication networks, interfaces have been standardized between different layers. Interface abstractions allow developments in each layer independent of the rest of the system. This approach allowed systems to be composed of independently developed components, opening opportunities for innovation and rapid proliferation of technology and the development of the Internet. In the IoT space, existing tools, practices, and standards do not support routine modular design and development. Standardized architectures, interfaces, models, and abstractions are needed to support agile development, verification and validation, interoperability, and innovation in IoT systems. The global nature of the IoT points to the need for standards which include graduated or scalable levels of trust. Additionally, further research is needed for legacy equipment management, particularly in industrial settings. Some existing IoT devices, particularly in industrial settings, are rarely, if ever, rebooted or patched. Research is needed for security technologies that protect such long-lived devices.

Standards

Standards provide a basis for the interoperability that is the essence of the IoT value proposition. There are several types of interoperability, including technical, syntactical, semantic, organizational, static, and dynamic. All of these forms of interoperability are needed to effectively integrate IoT into NS/EP systems and operations.

IoT technologies supporting NS/EP systems should be based on open architectures to maximize interoperability among heterogeneous systems and distributed resources, including providers and consumers of information and services, whether human beings, software, smart objects or devices. Thus, standards organizations should develop common NS/EP security reference models, architectures, and interfaces for IoT systems.

Standards that define the technical and logical conditions that govern the interconnections and the interfaces by which the information is transferred will need to be adopted to enable the

desired level of interoperability. Standards will need to be developed for data encoding, air interfaces, testing, security, power use and dissipation, security and other functions. The Federal Government will need to be involved in standard setting groups (national and international) to facilitate the development of standards for IoT systems supporting NS/EP.

Identification, Security and Privacy Technologies and Practices

Global communications networks are evolving to accommodate the emerging IoT technology deployments. However, further research is needed in the development, convergence, and interoperability of technologies for identification and authentication to enhance operation at a global scale.

Given privacy and confidentiality concerns research and testing is needed on the deployment of technologies that enable identity and anonymity. For example, a device could be attested to be part of a group without revealing unique identity properties. Similarly, the technology could be used to verify that a person is part of a group (e.g., licensed driver) without revealing unique identity. Exploration of the appropriate certificate authority for such capabilities should also be undertaken.

Unanticipated consequences regarding the deployment of IoT systems may result from the massive volume of data produced by many different sources, and the increasing inter-connections and data retention. In the IoT environment, every node could be connected to the global Internet and be able to communicate with other nodes, creating new security and privacy concerns, such as confidentiality, authenticity, and integrity of data collected and exchanged by IoT networks.

Network Management Technologies

The design and implementation of IoT networks that interconnect within the national ecosystem pose several challenges related to the real time nature of operations, reliability, security requirements, applications, and interworking of heterogeneous systems. The network management systems for IoT networks will have to monitor parameters such as traffic flow and congestion, stability, and availability of the large-scale real time systems and system-wide security. Network management technologies will need visibility into the underlying networks and check the processes that run on them, regardless of device, protocol, or geographic location. A particular focus of the research should be the use of predictive analytics in network operation optimization and cyber attack detection.

2.2.3.3 International Implications

IoT is a global phenomenon and requires global engagement in research and development, and in standards development. The United States needs to be actively engaged in international activities to keep pace and lead with advancements and evolving standards.

As mentioned previously, the IoT brings the benefit of global reach enhanced by the speed of M2M operations. Yet, M2M's current standards lack a comprehensive end-to-end view for M2M ecosystems. Multiple standards bodies exist; however, standards tend to be very specific and focused on a particular technology, lack detail, and do not address end-to-end view. For

example, the Third Generation Partnership Project Security Architecture 3 is focused on security of interfaces between connected devices with Subscriber Identity Module (e.g., Universal Integrated Circuit Card) and mobile access technologies.[19] The European Telecommunications Standards Institute, as a member of oneM2M, is taking a top-down approach to defining service creation to the device. They are defining requirements for network, access technologies, and devices that are actually under the scope of other standards organizations or forums. The actual influence they will have in these areas is still to be determined. A comprehensive protocol and implementation agnostic standard would help make device certifications easier to develop and recognize.

For global connectivity, connecting M2M mobile devices with different operators and across borders is challenging and requires an integrated solution. These challenges include deployment, provisioning, re-provisioning geolocation and remote management of the SIM. Additionally, automating billing, reporting, support, and operational management processes differ with carriers and introduce more complex requirements to the host platform provider. Presently, over-the-air (OTA) solution cover backend secure data generation and management and offer the highest level of security but these platforms are designed for local service that is within network. OTA will not always work in roaming services and may not meet regional regulations, performance standards, and consumer needs. In order to achieve the full benefits and potential of IoT, and in light of its global reach, there is a need to have interoperable technologies and policy discussions in the appropriate international fora.

3.0 FINDINGS

The NSTAC's examination has revealed several findings related to the IoT in three areas: (1) IoT technology and unprecedented effects; (2) governance of IoT; and (3) institutional support and structure. The section in which the finding is first discussed appears in parenthesis following each finding.

3.1 IoT Technology/Unprecedented Effects

- The cybersecurity implications related to IoT are enormous. (Section 2.1)
- The IoT is already impacting society. The vast growth in deployments of and uses for IoT technologies ranges from the individual citizen to the Nation (through initiatives such as Smart Grid, Smart Cities, and Smart Transportation). (Section 2.1)
- Consensus estimates suggest that at least 50 billion devices will be in use by 2020, resulting in more than $8 trillion in global economic revenue. (Section 1.0)
- The line between consumer and industrial devices continues to blur, with consumer devices used – intentionally or not—in ways that affect NS/EP. The strong growth in interconnected, potentially adaptive devices implies a larger cybersecurity attack surface with potentially cascading adverse effects in both the cyber and physical domains. (Section 2.2.1.3)

[19] 3GPP: The Mobile Broadband Standard. Available at: http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

- The massive deployment of IoT devices as part of interconnected ecosystems, including consumer and national security systems, is driving the need to adjust cybersecurity policies to cover, respond, detect, and protect. (Section 2.1)
- IoT represents a convergence, or perhaps a collision, of IT and OT. To this point, the two disciplines have approached cybersecurity differently. IT security involves patches and frequent updates and the ability to take systems offline as needed, while OT security is largely based on obscurity and specialization, in large part because of the need for systems to remain online, whether compromised or not. This disconnect creates gaps that attackers could exploit. (Section 2.2.1.3)
- The diverse, heterogeneous, and decentralized nature of the IoT creates opportunities for new thinking on approaches to provide end-to-end ecosystem security and resiliency where decisions can be made autonomously, and coordinated to enable collaborations with multiple jurisdictions to enable near real-time responses to NS/EP events. The increased attack surface of the IoT can be leveraged to increase situational awareness and points of control in such processes. (Section 2.2.1.4)

3.2 Governance of IoT

- Innovation and adoption of IoT technology are outpacing the development of IoT governance structures and related policies. This appears to be true at both the national and global levels. (Section 2.2.1.4)
- IoT is not addressed in a number of national cybersecurity strategic guidance documents; thereby, leaving roles, responsibilities, authorities and resourcing unclear relative to maximizing benefit and minimizing risk associated with IoT for NS/EP. (Section 2.2.2.1)
- There is no agreement on what comprises the boundaries of IoT (versus CPS, IT, OT), complicating the efforts to create IoT policy. (Section 2.2.1.4)
- The scale, degree of interconnectivity, and speed of action associated with IoT creates opportunities for new thinking on approaches and development of security guidelines to provide end-to-end ecosystem security and resiliency. Coordination and collaboration across multiple jurisdictions could enable near-real time response to NS/EP events. (Section 2.2.1.4)
- Current IoT devices are unable to leverage existing or planned NGN-PS features for GETS/WPS PIN validation. To support IoT, NS/EP policy should consider M2M, end-point NGN-PS authorization, session establishment, authentication, and completion. (Section 2.2.2.4)

3.3 Institutional Support & Structure

- There is no accepted definition of the IoT and it is often referred to using different terms, including Industrial Internet and CPS. (Section 2.1)
- The speed of innovation and deployment of IoT has outpaced traditional institutional support and organizational structures, such as education, awareness programs, research and development that would normally enhance technology deployments (Section 2.2.1.3); resulting in the following:

  - Shortage of trained personnel with IoT related cybersecurity skills and knowledge, including leaders and decision makers in both private and public sector.
  - R&D funding not clearly allocated, coordinated and prioritized to cover IoT cybersecurity challenges, particularly in the context of NS/EP.

- The emergence of IoT and the convergence of IT and OT demand experts who understand and can respond effectively to these new challenges. Academic programs that integrate core concepts and the implications of new interdependencies are needed, as are training programs for practicing professionals in both IT and OT and in the development of future IoT (Section 2.2.3.1).
- National cybersecurity strategic documents that were meant to be enduring and mission focused are silent with regard to IoT (Section 2.2.2.1).
- The enormous growth in deployment and interconnectivity of IoT devices in the private sector offers opportunities for market forces to drive increased security, privacy, and resilience (Section 2.2.3.1).
- IoT is a global phenomenon and requires global engagement in R&D and standards development. In order to achieve the full benefits and potential of IoT, and because of its global reach, there is a need to have interoperable technologies and policy discussions in the appropriate international fora (Section 2.2.3.3).

4.0 CONCLUSION

There is a small and rapidly closing window to grasp the opportunities of IoT in a way that maximizes security and minimizes risk. If the Nation fails to do so, it will be coping with the consequences for generations. Many of the benefits of the IoT are already being realized, including increased efficiencies, early detection of faults, and improved reliability and resilience. But the rapid and massive connection of new devices brings with it risks, including new attack vectors, new vulnerabilities, and perhaps most concerning of all, the ability to use remote access to cause physical destruction.

The explosive growth and interconnectivity associated with IoT has created a NS/EP issue. Billions of IoT devices (e.g., sensors, processors, and actuators) that can communicate with each other, within a closed network, and sometimes across the broader Internet, can be incorporated directly into our Nation's critical infrastructure systems. Additionally, many personal and consumer devices will connect to networks that have some connectivity to critical systems, often unknowingly, thus creating new attack avenues for an adversary. Moreover, if history is any guide, the technology that underpins many personal devices will find its way into devices that are integrated into critical systems.

The cybersecurity problems the United States currently faces are, in some ways, analogous to the era when the protocols that govern the Internet were developed, in that security was not a significant consideration. At the time, the pervasive use of the Internet—for everything from commerce to global communications to life-sustaining functions—was not conceivable. Had the early designers of the Internet envisioned this, there is no doubt they would have placed a higher priority on security. Today, the Nation now stands on the edge of a similar revolution in how it

interacts with devices and how they will serve us; however if security is not included as a core consideration, there are very real consequences, both economically and to the safety of life. The next two to five years is the opportunity to get this right; after that, the Nation will be living with the consequences of inaction—and ruing another missed opportunity to insist upon security early in a technological wave.

5.0 RECOMMENDATIONS

In light of the rapid adoption of emerging technologies and the dynamic threat environment, immediate action is needed to address the dynamic IoT environment. The NSTAC found that existing governance, policy, and institutional support structures are not well-equipped to facilitate the rapid changes needed; therefore, NSTAC suggests the first three recommendations be acted upon within 90 days. Based on the authorities and responsibilities established by EO 13618, Assignment of National Security and Emergency Preparedness Communications Functions, the NSTAC recommends that the President execute the following recommendations:

1. Direct the Department of Commerce, specifically NIST, to develop a definition of IoT for use by departments and agencies to be used during assessments related to the IoT.

2. Direct the Office of Management and Budget to require Federal departments and agencies to:

    a. Conduct an internal assessment to document IoT capabilities that currently support and/or planned for support of NS/EP functions. These assessments must consider interconnections and interdependencies that may be introduced and the associated risks and benefits with respect to NS/EP.

    b. Develop contingency plans to identify and manage security issues created by current and future IoT deployments within the Government. The plans should recognize that IoT devices and their potential uses will continually evolve as well as anticipate an environment that cannot be fully secured because of the dynamic nature of the IoT and the potential threat.

3. Create an IoT interagency task force that coordinates with existing organizational bodies to foster balanced perspectives between security, economic benefits, and potential risks. At a minimum, participants should include the Department of Commerce, Department of Homeland Security, and Department of Defense. The task force will set milestones for completion of the following activities that are reflective of the urgency of need to address the risks that ongoing deployments of IoT pose to NS/EP.

    a. Identify the gaps between security practices and emerging technologies to address the unique risks posed by IoT on NS/EP and develop plans for how to incentivize development of security innovations to address the gaps.

    b. Direct the update of Federal strategic documents to consider the security aspects of the explosive growth of and reliance upon IoT devices. Examples include the National Strategy to Secure Cyberspace, the Comprehensive National

Cybersecurity Initiative, and Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program.

c. Direct the update of existing awareness and training programs. The focus of the awareness should be to inform the public, as well as leaders and decision makers (private and public, including legislators), about both the benefits and risks of the rapid adoption of IoT and, thereby, encourage a culture of security around IoT device use and development. Role-specific programs should be considered for those involved in the design, development, production, procurement, and operation of NS/EP systems.

d. Encourage and incentivize academia to develop curricula focused on: (i) IoT, and the associated security challenges; and (ii) the convergence of the IT and OT disciplines, in order to educate future professionals engaged in the design, administration, or security of NS/EP systems.

e. Encourage engagement in appropriate international forums for standards and policy development.

4. Convene and facilitate a Government and industry standing body to coordinate, collaborate and leverage the various industry IoT consortia to develop, update, and maintain IoT deployment guidelines to manage cybersecurity implications and risks. These guidelines should include the integration of IoT into systems that support NS/EP functions and highlight the gaps between risks the market will address and national security risks, which markets are not intended to address and are for use as part of the acquisition, procurement, and operations procedures. The result should enable an adaptive set of guidelines, focused cybersecurity and resiliency of the ecosystem that changes with the risk in a timely manner based on a continuous collaborative process. The executive agent of this standing body must have authority and oversight to enforce agreed-to deployment guidelines across governmental agencies and departments.

5. Direct the NS/EP Communications Executive Committee to: (1) review and recommend updates through the PPD-1 process on priority schema to account for and enable priority on all forms of next generation networks communications (e.g., voice, video, data) for NS/EP and public safety communications; (2) appropriately account for the impact the growth of IoT and IoT-related data associated with NS/EP communications; and (3) develop, in conjunction with the private sector, updates to NS/EP programs including GETS, WPS, TSP, and SRAS.

6. Direct the Office of Science and Technology Policy to review current R&D investment and recommend future R&D funding for IoT security. Funding will help to understand the potential risks to NS/EP functions associated with IoT in an interconnected ecosystem, including IoT architectures, network management, privacy, and device identification and authentication in a manner that allows for productivity, growth, and innovation. Measure improvements in adoption and implementation of new technologies from the research execution with linkages to national priorities and interests and ensure that existing, similar recommendations are appropriately executed.

As recommendations are considered and implemented, it will be important to: (1) establish metrics to measure and monitor the effectiveness of the recommendations; (2) incorporate IoT technology in a manner that minimizes risk; (3) incorporate IoT in current education and awareness programs; and (4) ensure IoT-related R&D projects are addressing evolving cybersecurity challenges. The NSTAC believes these actions will help maximize security and resiliency within the IoT ecosystem.

APPENDIX A: MEMBERSHIP

SUBCOMMITTEE MEMBERS

Mr. William Swanson, Chair

Mr. William Russ, IoTS Working Group Co-Chair
Mr. Jeffrey Greene, IoTS Working Group Co-Chair

Akamai Technologies, Incorporated	Mr. David Belson
AT&T, Incorporated	Mr. T. Brooks Fitzsimmons
Avaya, Incorporated	Dr. Margaret Leary
CenturyLink, Incorporated	Ms. Kathryn Condello
Ciena Corporation	Mr. David Krauss
Communications Technologies, Incorporated	Mr. Milan Vlajnic
CSC	Mr. Guy Copeland
Ericsson, S.A.	Ms. Louise Tucker Mr. Stephen Hayes
FireEye, Incorporated	Mr. Tony Cole
Frontier Communications Corporation	Mr. Michael Saperstein
General Services Administration	Ms. Maria Roat
Harris Corporation	Mr. Michael Higgins Mr. Stephen Reese
Homeland Security Studies and Analysis Institute	Dr. Matthew Fleming
Institute for Defense Analyses	Dr. Elizabeth McDaniel
Iridium Communications, Incorporated	Mr. David Wigglesworth
Isis Defense	Mr. Marvin Wheeler
Juniper Networks, Incorporated	Mr. Robert Dix

Lockheed Martin Corporation	Mr. Macy Summers
McAfee, Incorporated	Mr. Patrick Flynn Ms. Lorie Wigle
Microsoft Corporation	Ms. Angela McKay
Neustar, Incorporated	Ms. Terri Claffey
Palo Alto Networks, Incorporated	Mr. William Gravell
Raytheon Company	Mr. Michael Daly Mr. Jon Goding
Rockwell Collins, Inc.	Mr. Ken Kato
Sprint Corporation	Mr. Kevin Frank Mr. Scot Kight
TE Connectivity, Ltd.	Mr. William Weeks
Verizon Communications, Incorporated	Mr. Marcus Sachs
Vonage Holdings Corporation	Mr. Alistair Sloan

Subject Matter Experts

AT&T, Incorporated	Ms. Rosemary Leffler
CenturyLink, Incorporated	Mr. Michael Glenn Mr. Robert Morrill
General Services Administration	Ms. Carol Williams
Juniper Networks, Incorporated	Mr. James Bean
Microsoft Corporation	Mr. Paul Mitchell Ms. Carolyn Nguyen

Management Support

NSTAC Designated Federal Officer	Ms. Helen Jackson
Alternate NSTAC Designated Federal Officer	Ms. Deirdre Gallop-Anderson

Booz Allen Hamilton	Ms. Ursula Arno Ms. Elizabeth Voeller
Total Systems Technologies Corporation	Mr. Chad E. Kirk

APPENDIX B: ACRONYMS

CIKR	Critical Infrastructure and Key Resources
CPS	Cyber-Physical Systems
DHS	Department of Homeland Security
DNI	Director of National Intelligence
EO	Executive Order
FIPPS	Fair Information Practice Principles
GETS	Government Emergency Telecommunications Service
ICS	Industrial Control Systems
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
M2M	Machine-to-Machine
MS-ISAC	Multi-State Information Sharing and Analysis Center
NGN-PS	Next Generation Network Priority Services
NICE	National Initiative for Cyberspace Education
NS/EP	National Security and Emergency Preparedness
NIST	National Institute of Standards and Technology
NSTAC	National Security Telecommunications Advisory Committee
OEC	Office of Emergency Communications
OT	Operational Technology
OTA	Over-the-Air
PIN	Personal Identification Number
R&D	Research and Development
SCADA	Supervising Control and Data Acquisition
SRAS	Special Routing Access Services
SWOT	Strengths, Weaknesses, Opportunities, and Threats
TSP	Telecommunications Service Priority
WPS	Wireless Priority Service

APPENDIX C: GLOSSARY

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

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

Capacity: The information carrying ability of a telecommunications facility. What the "facility" is determines the measurement (e.g., you might measure a data line's capacity in bits per second). (Newton's Telecom Dictionary)

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

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

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

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

Critical Infrastructure and Key Resources (CIKR): Elements that support the essential functions and services that underpin American society. (DHS.gov)

Data Aggregation: Compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

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

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

Fair Information Practice Principles: A set of eight principles that form the basis of the Department of Homeland Security's privacy compliance policies and procedures governing the use of personally identifiable information. (DHS.gov)

Government Emergency Telecommunications Service (GETS): Provides national security and emergency preparedness (NS/EP) personnel a high probability of completion for their phone calls when normal calling methods are unsuccessful. It is designed for periods of severe network congestion or disruption, and works through a series of enhancements to the public switched telephone network. GETS is in a constant state of readiness. Users receive a GETS "calling card" to access the service. This card provides access phone numbers, Personal Identification Number (PIN), and simple dialing instructions. (DHS.gov)

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

Identity Validation: Tests enabling an information system to authenticate users or resources. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Industrial Control Systems: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

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

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

Interoperability: The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together for mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility for use in services outside the direct control of the issuing assigner. (International Organization for Standardization Technical Committee 46/Subcommittee 9)

Long Term Evolution (LTE): The access part of the Evolved Packet System. The main requirements for the new access network are high spectral efficiency, high peak data rates, short round trip time, and frequency flexibility. (3GPP.org) LTE is the standard created and adopted by 3GPP through its Release 8 regarding fourth generation (4G) cellular wireless telecommunications. 4G is based upon an all IP packet switched network that supports mobile broadband access as well as multi-media applications with high data rates and low latencies utilizing spectrum efficiency by smooth handoffs and seamless roaming across multiple networks. LTE has been accepted and adopted by national and international communities as the foundation for future mobile telecommunications. (http://transition.fcc.gov/pshs/docs/LTE_Info_Sheet_09082010.pdf)

Machine-to-Machine (M2M): Technologies that enable computers, embedded processors, smart sensors, actuators and mobile devices to communicate with one another, take measurements and make decisions - often without human intervention. (Machine to Machine Technology in Demand Responsive Commercial Buildings)

Next Generation Network Priority Services: A National Communications System program to define and deploy priority voice communications in the next generation packet- switched network environment. (DHS.gov)

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

Personally Identifiable Information: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Government Accountability Office Report 08-536)

Reliability: A measure of how dependable a system is once you actually use it. (Newton's Telecom Dictionary)

Resilience: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (PPD-8: National Preparedness)

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

Security: A way of insuring data on a network is protected from unauthorized use. Network security measures can be software-based where passwords restrict users' access to certain data files or directories. This kind of security is usually implemented by the network operating system. Audit trails are another software-based security measure, where an ongoing journal of what users did what with what files is maintained. Security can also be hardware-based, using more traditional lock and key. (Newton's Telecom Dictionary)

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

Spectrum: A continuous range of frequencies, usually wide in extent within which waves have some specific common characteristics. (Newton's Telecom Dictionary)

Supervisory Control and Data Acquisition (SCADA Systems): A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (delays, data integrity, etc.) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated. (NIST Glossary of Information Security Terms – NISTIR 7298 Revision 2)

Survivability: A property of a system, subsystem, equipment, process, or procedure, that provides a defined degree of assurance that the device or system will continue to work during and after a natural or man-made disturbance (e.g., nuclear attack). This term must be qualified by specifying the range of conditions over which the entity will service, the minimum acceptable level of post-disturbance functionality, and the maximum acceptable outage duration. (Newton's Telecom Dictionary)

Telecommunications Service Priority (TSP): A regulatory, administrative, and operational system authorizing and providing for priority treatment (i.e., provisioning and restoration) of national security and emergency preparedness (NS/EP) telecommunications services. (DHS.gov)

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

Wireless Priority Service (WPS): A priority communications service for improving call completion capabilities for authorized NS/EP cell phone users. In the event of congestion in the wireless network, an emergency call using WPS can queue for the next available channel. All WPS (and GETS) calls will receive priority during access, transport, and egress to a wireless mobile on a WPS carrier, even if the terminating mobile is not subscribed to WPS. WPS calls do not preempt calls in progress or deny the general public's use of the radio spectrum. (GETS/WPS Program Management Office, DHS.gov)

APPENDIX D: BIBLIOGRAPHY

Adler, Emily. "Here's Why 'The Internet Of Things' Will Be Huge, And Drive Tremendous Value For People And Businesses." *Business Insider*, December 7, 2013. Available: http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "Smart Objects" to "Social Objects": The Next Evolutionary Step of the Internet of Things." IEEE Communications Magazine, pp. 97-105, January 2014.

Bent, Kristin. "CES 2014: Cisco Ups Internet of Everything Opportunity to $19 Trillion." *CRN*, January 8, 2014. Available: http://www.crn.com/news/networking/240165224/ces-2014-cisco-ups-internet-of-everything-opportunity-to-19-trillion.htm?cid=rssFeed.

Brown, Greg. "Risk and the Internet of Things." SANS, ZIP File, October 30, 2013. Available: https://files.sans.org/summits/internet13/.

Cannady, Stacy. "Just Trust Me! Internet Enabled Devices with Integrity." SANS, ZIP File, October 30, 2013. Available: https://files.sans.org/summits/internet13/.

Chandna, Asheem. "The Internet of Things – Trends and Opportunities." SANS, ZIP File, October 2013. Available: https://files.sans.org/summits/internet13/.

Clapper, James R., Statement to the Senate Select Committee on Intelligence, Worldwide Threat Assessment of the U.S. Intelligence Committee, January 29, 2014. Available: http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf

Cisco, "Cisco Study Says Internet of Everything Can Create Savings, Increase Productivity and Revenue for Governments Globally, While Improving Citizen Benefits." Cisco, January 8, 2014. Available: http://newsroom.cisco.com/release/1308288.

Clay, Jon, "Internet of Things – Insecurity Case Studies and Insights." SANS Institute, October 30, 2013. Available: https://files.sans.org/summits/internet13/.

Conti, Marco, Sajal K. Dasb, Chatschik Bisdikian, Mohan Kumarb, Lionel M. Ni, Andrea Passarella, George Roussos, Gerhard Tröster, Gene Tsudik, and Franco Zambonelli. "Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence." Pervasive and Mobile Computing Journal. Volume 8, Issue 1, February 2012, Pages 2-21.

Department of Energy. "Energy Department Release New Guidance for Strengthening Cybersecurity of the Gird's Supply Chain." April 28, 2014. Available: http://energy.gov/articles/energy-department-releases-new-guidance-strengthening-cybersecurity-grid-s-supply-chain.

Department of Homeland Security, Cyber Security Division- Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC). "Linking the Oil and Gas Industry to Improve Cyber Security." Available: https://www.dhs.gov/csd-logiic.

Department of Homeland Security, Idaho National Laboratory, David Kuipers and Mark Fabro. "Control Systems Cyber Security: Defense in Depth Strategies." May 2006. Available: http://www.inl.gov/technicalpublications/Documents/3375141.pdf.

Department of Homeland Security, National Cyber Security Division, Control Systems Security Program. "Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies." October 2009. Available: http://ics-cert.us-cert.gov/sites/default/files/recommended_practices/Defense_in_Depth_Oct09.pdf.

Department of Homeland Security, National Protection and Programs Directorate. *Cybersecurity Insurance Workshop Readout Report*. November 2012. Available: https://www.dhs.gov/sites/default/files/publications/cybersecurity-insurance-read-out-report.pdf.

Department of Homeland Security, National Protection and Programs Directorate. *Cyber Risk Culture Roundtable Readout Report*, May 2013. Available: https://www.dhs.gov/sites/default/files/publications/cyber-risk-culture-roundtable-readout_0.pdf.

Dhanjani, Nitesh, "Abusing the Internet of Things." SANS Institute, October 30, 2013. Available: https://files.sans.org/summits/internet13/.

EO 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*. July 7, 2012. Available: http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-.

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

Geer, Dan, "Heartbleed as Metaphor." *Lawfare Blog*, April 21, 2014. Available: http://www.lawfareblog.com/2014/04/heartbleed-as-metaphor/.

Goodin, Dan. "New Linux Worm Targets Routers, Cameras, "Internet of Things" Devices." *ArsTechnica*, November 27, 2013. Available: http://arstechnica.com/security/2013/11/new-linux-worm-targets-routers-cameras-internet-of-things-devices/.

Hewlett-Packard. *Internet of Things Research Study: 2014 Report*. Available: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en.

Higginbotham, Stacey. "The Internet of Things Needs a New Security Model. Which One Will Win?" *Gigaom*, January 22, 2014. Available: http://gigaom.com/2014/01/22/the-internet-of-things-needs-a-new-security-model-which-one-will-win/.

Hinchcliffe, Dion. "Is the Internet of Things strategic to the enterprise?" *ZDNet*, May 31, 2014. Available: http://www.zdnet.com/is-the-internet-of-things-strategic-to-the-enterprise-7000030068/

Holdman, Michael. "Why the Industrial Internet Needs a Secure "Push" Messaging Solution." January 1, 2014. Available: http://mholdmann.wordpress.com/2014/01/01/why-the-industrial-internet-needs-a-secure-push-messaging-solution/?goback=%2Egde_3045583_member_5824226377779396612#%21

Industrial Control Systems Cyber Emergency Response Team. Daktronics Vanguard Default Credentials. June 6, 2014. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A

IO Data Centers, LLC, "Internet of Everything," July, 2014.

IO Data Centers, LLC, "Securing the Grid, Opportunities and Risks in Operational Technology," July, 2014.

Kennedy, Ian. "A Trillion Endpoints: Disruptive Innovation, Smart Objects, and the Internet of Things, Final Briefing." Cisco, 2013. Available: http://coseners.net/wp-content/uploads/2013/12/A-trillion-endpoints-v12-public.pdf.

Kovacs, Eduard. "Default Password Exposes Digital Highway Signs to Hacker Attacks." *Security Week*, June 6, 2014. Available: http://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks

Krebs, Brian. "They Hack Because They Can." *Krebs on Security*, June 5, 2014. Available: http://krebsonsecurity.com/2014/06/they-hack-because-they-can/

Langner, Ralph. "Stuxnet's Secret Twin: The Real Program to Sabotage Iran's Nuclear Facilities Was Far More Sophisticated than Anyone Realized." *Foreign Policy*, November 19, 2013. Available: http://www.foreignpolicy.com/articles/2013/11/19/stuxnets_secret_twin_iran_nukes_cyber_attack?print=yes.

Lee, Michael. "M2M and the Internet of Things: How secure is it?" *ZDNet*, January 10, 2013. Available: http://www.zdnet.com/m2m-and-the-internet-of-things-how-secure-is-it-7000008389/.

Lemos, Robert. "Cyber-Attackers to Focus on Internet of Things in 2014: IT Experts." eWeek, December 31, 2013. Available: http://www.eweek.com/security/cyber-attackers-to-focus-on-internet-of-things-in-2014-it-experts.html.

Liebowitz, Matt. "Hacker Says He Breached Texas Water Plant Network." *NBC News*, November 21, 2011. Available: http://www.nbcnews.com/id/45394132/ns/technology_and_science-security/t/hacker-says-he-breached-texas-water-plant-network/#.VFfBQVeeKO4

LOGIIC Consortium. "The LOGIIC Consortium Announces its Initiative to Improve the Security of Oil and Gas Critical Infrastructure." *LOGIIC Consortium News Release*, April 21, 2010. Available: https://logiic.automationfederation.org/public/default.aspx.

Macmanus, Richard. "The Compelling (or Creepy) M2M World of Verizon Wireless." *ReadWrite*, July 13, 2011. Available: http://readwrite.com/2011/07/13/m2m_world_of_verizon_wireless.

Maucione, Scott. "Experts Reveal the Future of Mobility." *FedScoop*, February 28, 2014. Available: http://fedscoop.com/experts-reveal-future-mobility-mobilegov-summit/.

McMillan, Robert. "It's Crazy What Can Be Hacked Thanks to Heartbleed." *Wired*, April 28, 2014. Available: http://www.wired.com/2014/04/heartbleed_embedded/.

Mills, Elinor. "Hacker Says He Broke Into Texas Water Plant, Others." *Cnet*, November 18, 2011. Available: http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/

MIT Technology Review, Weekly Computing Newsletter, January 23, 2014. Available: http://newsletters.technologyreview.com/email/weekly/computing/20140123/.

National Intelligence Council, "Disruptive Civil Technologies, Six Technologies with Potential Impacts on US Interests out to 2025." April 2008.

National Research Council. "Professionalizing the Nation's Cybersecurity Workforce: Criteria for Decision-Making." Washington, DC: The National Academies Press, 2013. Available: http://www.nap.edu/catalog.php?record_id=18446.

National Security Telecommunications Advisory Committee. *NSTAC Report to the President on Secure Government Communications*, August 20, 2012. Available: https://www.dhs.gov/publication/2013-nstac-publications.

Ning, Huansheng, Hong Liu, and Laurence T. Yang, "*Cyberentity Security in the Internet of Things*." IEEE Computer Society, pp: 46-53, April 2013. Available: http://www.computer.org/csdl/mags/co/2013/04/mco2013040046-abs.html.

Perkins, Earl. "Securing the Internet of (Every)Things." SANS Institute, October 30, 2013. Available: https://files.sans.org/summits/internet13/.

Perlroth, Nicole. "Hackers Lurking in Vents and Soda Machines." *New York Times*, April 7, 2014, Available:http://www.nytimes.com/2014/04/08/technology/the-spy-in-the-soda-machine.html?hp&_r=0.

PR Newswire. "The Center for Public Policy Innovation Hosts Policy Forum on the 'Internet of Everything'," *Reuters*, November 7, 2013. Available: http://www.reuters.com/article/2013/11/07/cppi-ioe-forum-idUSnPnDC4sct0+160+PRN20131107.

Rath, John. "Cisco: 2014 Will Be Key Tipping Point for Internet of Everything." Data Center Knowledge, January 8, 2014. Available: http://www.datacenterknowledge.com/archives/2014/01/08/ciscos-transformational-vision-for-the-internet-of-everything/.

Ravindranath, Mohana. "Cisco CEO at CES 2014: Internet of Things is a $19 Trillion Opportunity." *The Washington Post*, January 8, 2014. Available: http://www.washingtonpost.com/business/on-it/cisco-ceo-at-ces-2014-internet-of-things-is-a-19-trillion-opportunity/2014/01/08/8d456fba-789b-11e3-8963-b4b654bcc9b2_story.html.

Ravindranath, Mohana. "Intel, Cisco, IBM Collaborate on Internet of Things." *The Washington Post.* March 27, 2014. Available: http://www.washingtonpost.com/business/on-it/intel-cisco-ibm-collaborate-on-internet-of-things/2014/03/27/b3fdae10-b446-11e3-8020-b2d790b3c9e1_story.html.

Ravindranath, Mohana. "Internet of Things: After the Cloud: Say Hi to "Fog Computing." *The Washington Post*, February 2, 2014. Available: http://www.washingtonpost.com/business/economy/it-news-briefs-cisco-is-developing-fog-computing-tablet-sales-reach-2171million/2014/01/31/73df313c-8845-11e3-916e-e01534b1e132_story.html.

Schneier, Bruce. "The Internet of Things Is Wildly Insecure — And Often Unpatchable." *Wired*, January 6, 2014. Available: http://www.wired.com/opinion/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

Stouffer, Keith, Joe Falco and Karen Scarfone. "Guide to Industrial Control Systems (ICS) Security." National Institute of Standards and Technology, Special Publication 800-82. June 2011. Available: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf.

Thibodeau, Patrick. "Government Use of Sensors May be a Portal for Connected Devices." *ITNews*, January 29, 2014. Available: http://m.itnews.com/wireless/73721/internet-things-five-words-sensor-monkey-radio-cloud-paris?source=ITNEWSNLE_nlt_itndaily_2014-01-29.

Vance, Ashlee. "Behind the 'Internet of Things' Is Android—and It's Everywhere." *Bloomberg Businessweek*, May 30, 2013. Available: http://www.businessweek.com/articles/2013-05-29/behind-the-internet-of-things-is-android-and-its-everywhere.

Verizon Communications, Inc., *Data Breach Investigations Report 2014.* Available: http://www.verizonenterprise.com/DBIR/2014/.

Verizon Communications, Inc., "Security of Large Technical Systems," February, 2014.

Walsh, Larry. "Cisco: Internet of Things is Now a $19tn Opportunity." *CRN*, January 8, 2014. Available: http://www.channelweb.co.uk/crn-uk/news/2321732/cisco-internet-of-things-is-now-a-usd19tn-opportunity.

Wind River. "Tapping M2M: The Internet of Things." *ZDNet*, 2014. Available: http://www.zdnet.com/topic-tapping-m2m-the-internet-of-things/.

Wisniewski, Chester. "Interview with SCADA hacker pr0f about the state of infrastructure security." Naked Security, November 22, 2011. Available: http://nakedsecurity.sophos.com/2011/11/22/interview-with-scada-hacker-pr0f-about-the-state-of-infrastructure-security/

Work, Robert O. and Shawn Brimley, *20YY: Preparing for War in the Robotic Age*, Final Report. Center for a New American Security, January 22, 2014. Available: http://www.cnas.org/20YY-Preparing-War-in-Robotic-Age#.UuCLXxAo7rc.

APPENDIX E: AREAS OF FOCUS

In the *NSTAC Industrial Internet Scoping Report*, four areas of the IoT were identified to help shape its research effort: security, operations, design, and policy. Each focus area of the IoT is described in detail below and was used to inform the report's findings and recommendations.

I. Security

In its fullest implementations, the IoT poses some unique security challenges for national security and emergency preparedness (NS/EP), including:

- The diversity, heterogeneity, and sheer number of devices that are deployed and interconnected, potentially across multiple sectors and with global reach. Multiple classes of devices will be deployed, ranging from those with extremely limited capabilities, to those that can adapt their behaviors and functionalities to the environments and interactions around them.
- The majority of these devices will be embedded into environments with older legacy systems that cannot be easily updated and managed.
- The ecosystems and associated data generated and processed may be under multiple jurisdictions.
- The increased attack surface and the near-impossibility of securing the environments would imply that at any given time, some number of devices and systems are compromised.
- The IoT will include systems that can operate autonomously and independently in response to data input, faster than humans can intervene or comprehend, and may lead to cascading effects across multiple ecosystems.

Security frameworks designed to address the IoT implications on NS/EP should take these challenges into consideration, in addition to other more traditional security concerns. Essential principles of such frameworks would need to include mechanisms that can establish the following:

- Trustworthiness of the IoT ecosystems, including the infrastructure, devices, systems, data, algorithms and processes related to the overall ecosystems.
- Resiliency of the components and the ecosystems knowing that systems will be compromised.
- Considerations of user behaviors and needs in any risk mitigation processes.
- Partnership with industry to leverage best security practices and continued innovations, as well as create awareness of NS/EP impact on the IoT technologies being developed.

Such a security framework should also include mechanisms that can leverage the unprecedented volume and details of available information to help in predict and address these challenges.

II. Operations

The ultimate goal of IoT is to increase operational efficiency, power new business models, and improve quality of life. By connecting everyday objects and networking them together, simple data can be combined to produce usable intelligence.

Operationally, the IoT must function differently from the existing Internet. The IoT will be event-driven and triggered by sensors or signals indicating a state of change that has occurred. Thus IoT systems must respond to real-world events in order to control energy grids, manufacturing and processing plants, smart buildings, smart cities, smart homes, smart hospitals and smart transportation systems as well as monitor environmental parameters on land and sea. The IoT will have real-time operations, with ranges of time in which exchanges of information data must occur. Thus it will be important for NS/EP IoT systems to be able to interoperate and function among many IoT systems competing for the same scarce spectrum and or network capacity. It may even be important that NS/EP systems be dedicated to IoT networks within a group of networks that can manage the operational complexities within those networks.

Operationally, devices will be deployed in huge numbers, sometimes under difficult conditions, including battery-powered devices, with perhaps little storage capacity and processing power. It will be necessary for NS/EP IoT systems to operate within stable environments in order to ensure reliable end-to-end communications.

Given the need to ensure the reliability of NS/EP IoT systems, and the communications those systems carry, there may need to be a review of the spectrum bandwidth that IoT networks can use and whether the Government needs to consider giving priority to spectrum allocations for NS/EP IoT systems. As the communications industry increasingly looks to sharing spectrum to meet its growing spectrum needs, industry and Government will also need to consider how to design the databases that will facilitate this sharing.

III. Design

The emergence of the IoT raises questions about the design and architecture of pre-existing systems, and adds new dimensions to security issues for machine-to-machine (M2M) systems. Heterogeneous applications and systems will likely result in a lack of seamless interoperability and diverse architectures. Identification schemes such as electronic product codes will be impacted by new and innovative uses such as radio frequency identification. Certain design policies should be taken into consideration for NS/EP IoT systems[20]. At a minimum, security must be built into the design of any NS/EP system. NS/EP systems should also include:

- Operating systems with best practices, standards, requirements, and regulations, to address the mismatch in scale and responsiveness of IoT;
- Systems security standards and testing criteria developed by standards groups; and
- Restricted trust relationships as a subset of trust relationships and authorities.

[20] It is beyond the scope of this report to review optimal architecture reference models.

It is critical that NS/EP IoT systems be forward compatible to ensure compatibility with legacy systems. This will help to avoid fragmented systems which may hobble NS/EP communications. IoT systems must also be interoperable.[21] NS/EP IoT systems should be based on open architectures to maximize interoperability among heterogeneous systems and distributed resources, including providers and consumers of information and services, whether human beings, software, smart objects, or devices. Thus, NS/EP IoT systems need common NS/EP security reference models, reference architectures for future networks, Internet, IoT, and integration of legacy systems.

Classification and identification of the objects that are connected to the multiple networks making up the IoT is necessary with (1) naming schemes to identify objects; (2) addressing schemes to locate the objects; and (3) discovery mechanisms to find new and existing objects. Thus, NS/EP IoT systems need to be able to map to the devices, and create different taxonomies to identify risk, identity, and capability. These requirements have implications for trying to set up and manage a common NS/EP IoT system across industries, technologies, and geographies. Identification or mapping technologies will have to form the foundation of an NS/EP IoT system because the essential IoT system concept envisions a situation where everything, person or machine, communicates with everything that is attached to the system. Unique addressing will be required, possibly comparable to the URI scheme. Additionally, discovery services would provide sources of information for a particular object, identifying authenticated and authorized users.

Standards provide a basis for the interoperability that is the essence of the IoT value proposition. Standards that define the technical and logical conditions which govern the interconnections and the interfaces by which the information is transferred will need to be adopted to enable the desired level of interoperability. The standards can be classified according to the devices and things that they control. Standards will need to be developed for data encoding, air interfaces, testing, security, power use and dissipation, security and other functions. The Federal Government will need to be involved in standard setting groups to facilitate the development of standards for NS/EP IoT systems.

Finally, as Government considers current and future spectrum allocations, because most IoT systems will be wireless, it should consider NS/EP IoT system requirements. In particular it should consider what rules, if any, will need to change to accommodate the NS/EP and other IoT bandwidth and channel requirements. Spectrum standards will control various aspects of IoT applications including spectral bands used, power location, other aspects relating to interference and the device interface protocols.

As NS/EP IoT systems will need to be integrated to include legacy systems, NS/EP IoT systems should focus on replacement issues, and build in to the systems the lifespan of devices in order to ensure compatible policies across these systems. This forward compatibility will likely impact tax code provisions which, in turn, impact investment decisions. For example, replacement

[21] Interoperability is defined as the ability of two or more systems or components to exchange data and use information. There are many types of interoperability, to include technical, syntactical, semantic, organizational, static, and dynamic.

needs will drive capitalization of these systems, and current depreciation requirements in the tax code may be to be reviewed in order to handle NS/EP IoT system needs. In addition:

- NS/EP IoT systems will have to be rationalized with existing NS/EP programs including Next Generation Networks Priority Services (e.g., Wireless Priority Service, Government Emergency Telecommunications Service).
- Further, updated risk-based security performance measures should be developed to secure critical systems and components against cyber vulnerabilities.
- Carefully constructed threat models will have to be adopted that can help ensure that the right technical and nontechnical controls are in place to mitigate social harms and ensure the appropriate balance of interests.

The evolution of network systems is moving toward an environment where software will be controlling the network, and each of the things attached to the network. This world of "software defined things/software-defined everything" will require more rigorous software security standards to ensure the confidentiality, integrity, and availability of the IoT networks.

IV. Policy

The new advances from the global IoT systems raise public policy considerations for current and future NS/EP communications. The goals of NS/EP IoT systems will be to overcome the complex technical challenges of systems that interface cyber with physical, information technology with operational technology, and real-time sensor and actuator data systems riding on standardized Internet protocol-based networks, to achieve reliable, robust, scalable, secure, and dependable systems.

The IoT is developing rapidly. The current legal and technological public policies affecting the Internet are not immediately transferrable to an IoT where autonomous systems prevail. It is essential to examine what public policies should be in place to ensure that NS/EP IoT systems, with the appropriate characteristics of confidentiality, integrity and availability, can be deployed in this new environment.

Prioritization of services, and provisioning and restoration of facilities are hallmarks of NS/EP communications. Accordingly, the prioritization of services, the provisioning and restoration of IoT systems, and how these priorities can be addressed in an IoT environment are addressed in Section 2.2.2.4.

NS/EP IoT systems will need to be designed to be resilient. Autonomous M2M systems will need to include anomaly detection, with built-in ability for real-time predictive response. Resilience for IoT systems should include fault-tolerant network control, with evaluation of the limits of any defenses. NS/EP IoT systems will require novel approaches for detecting malicious actions, based on robust threat assessments and detection. A resiliency baseline for NS/EP IoT systems may need to be established in order to have a type of IoT device that can be used in an NS/EP IoT system. In addition, cost may be an issue.

NS/EP IoT systems will require a new security model. Security across the existing Internet security is too often an added-on feature. NS/EP IoT systems should have security built in and

address legacy and new hardware, and automatic software updates, including anomaly detection. Consideration should be given to establishing an Underwriters Lab for certification of specific securities policies.

NS/EP IoT systems will affect public safety. The IoT will connect huge numbers of machines to each other with agents or proxies acting for them. The effects of the actions taken by the machines could cause harm to society unless there is a way of limiting any extreme and unwarranted behavior. A requirement for an approach to safety for the IoT systems is needed. It will be necessary to ensure that autonomous machines always exhibit safe and rational behavior in line with some pre-set safety guidelines.

Further, NS/EP IoT systems are likely to be used in the emergency preparedness and response environments. Accordingly, the Federal Government should coordinate its implementation of NS/EP IoT systems with the First Responders Network Authority to ensure the interoperability and safety of IoT systems implemented for NS/EP systems.

Current legal and regulatory policies may not be immediately transferrable to the IoT. A future study will need to be conducted to address the gap between current legal and policy frameworks and new frameworks needed for the IoT systems.[22]

IoT has immense benefits for the gross domestic and national product of the Nation. In order to reap these benefits, and to enable the Government's use of the IoT for NS/EP communications, the Federal Government should consider adopting policies that can accelerate and improve the development of the IoT market. The Government could develop educational programs to both raise the awareness of IoT systems and support knowledge sharing. The Federal Government could also support and promote research and development for projects for identification, spectrum prioritization, and performance parameters of autonomous systems to protect the public safety.

Finally, as the IoT will operate in a global environment, it will require a globally unique scheme of identification. An identification scheme can be considered a critical resource, and any single point of failure could cause significant harm to the IoT infrastructure. To assure protection of this infrastructure, universally accepted rules governing such may need to be developed. Development and protection of an identifying scheme and its governing rules will require global cooperation. The Federal Government may want to encourage global cooperation to develop this scheme through existing global committees or establish a new international consortium of stakeholders to address this issue.

[22] Liability and responsibility for privacy, data protection, universal service, cybersecurity and other matters is beyond the scope of this report.

APPENDIX F: CASE STUDIES

We have been living in a world of networked devices for decades, but the broader implications of this connectivity—both good and bad—are still evolving, particularly as more of these devices are being connected to the broader Internet. The concept of a connected device does not necessarily connote an Internet connected device. In fact, many connected devices will not be connected to the Internet, but will instead only be part of closed networks. This may be by design, by choice, or by accident; it may be done for security reasons, or simply by chance. The fact that "connected" does not equal "Internet-connected" is a concept that cannot be lost as the adoption of the Internet of Things (IoT) accelerates because the decision whether to connect to the Internet is not one that should be left to chance. Internet connectivity can increase the utility of a device by enabling remote operation and data collection, yet at the same time this connection increases the security risk to the device and to any network the device touches. Thus the decision whether to connect should be made after a careful balancing of the equities, and with due consideration for incorporating security protocols if the decision is made to connect to the Internet.

What follows are several case studies that highlight both the positives and negatives of connecting networked devices to the Internet. These are real examples, drawn from open source reporting cited below. They demonstrate both the potential societal benefits of the IoT as well as the vulnerabilities in systems that are essential to our daily life. Collectively the case studies provide some context to the discussion of both the enormous benefits and the significant risks that the IoT will bring with it, discussed more fully in the body of this report.

North Carolina Highway Signs Compromised By a Foreign Hacker

In May 2014, a person believed to be a Saudi national and calling himself "Sun Hacker" compromised five overhead highway signs in North Carolina, changing them to read "HACKED BY SUN HACKER" and "HACK BY SUN HACKER TWITT (sic) WITH ME." Shortly after the messages appeared on the signs, a Twitter user going by the name Sun Hacker posted a tweet that described how he hacked the electronic sign system. Though individual road signs have been compromised and changed to warn of zombie attacks and other farcical threats, this is the first known case of a mass compromise of networked road signs. The Multi-State Information Sharing and Analysis Center (MS-ISAC) later reported that he compromised 11 signs in three states and that in one instance he altered the settings on system's modems, which forced technicians to reset them to their factory settings before they could regain access to the system. The MS-ISAC also said that Sun Hacker has previously shown an interest in the Internet of Things and has posted instructions on how to compromise IoT devices. The Department of Homeland Security's Industrial Control System Cyber Emergency Response Team also issued a statement warning companies that a particular highway message system was vulnerable to cyber attacks. Thankfully there were no traffic incidents reported as a result of this hack, but a

malicious actor with control over highway signage could cause major traffic problems and cause major disruptions, particularly during an emergency.[23,24,25]

Smart America Challenge Demonstrates the Utility of the Internet of Things

The Smart America Challenge was a White House Presidential Innovation Fellow project that brought together industries including manufacturing, healthcare, energy, and transportation to show how IoT devices could improve the US economy and the lives of American citizens. In December 2013, over 65 companies, Government agencies, and academic institutions organized 24 teams and in June 2014 each team presented its work in Washington D.C. Teams focused on different categories for their projects, and the projects ranged from developing a smart home that connects energy management, security, and healthcare to building smart roads that could improve both safety and traffic congestion. Other teams focused on security. One team looked at how to use the IoT to operate the power grid more effectively. The demonstrations highlighted the potential for significant societal benefit from IoT use and at the same time underscored the importance of a holistic view and approach regarding IoT security. Without an approach that considers the security implications of the IoT ecosystem, the massive new interconnections resulting from IoT device deployments will unnecessarily increase the attack surface and associated risk.[26]

Penetration of a Water Treatment Facility by a Foreign Hacker

In November 2011, a hacker calling himself "pr0f" and who appeared to be located outside the United States, posted screenshots of the graphical user interface of the control system of a water treatment plant in South Houston, Texas. Though he had full access to the control system, pr0f did not alter any of the settings nor impact the system in any way. He later claimed that he intentionally limited how much information he made public in order to protect the systems. The hacker said that he used the penetration to publicize how easy it is to access some systems that control essential services to thousands of people. pr0f made it clear that this was not a sophisticated intrusion, and he said that he is neither a security professional nor a control systems expert. He did not target South Houston specifically; instead, he began by using publicly available search engines to scan the internet for industrial control systems that had open internet connections. Once he located the system in question, he quickly determined that its standard configuration included a default user name and password. With this information in hand, pr0f simply logged into the system that had not changed its default credentials. Local officials

23 Department of Homeland Security, Industrial Control Systems Cyber Emergency Response Team. Alert: Daktonics Vanguard Default Credentials. June 6, 2014. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A

24 Kovacs, Eduard. "Default Password Exposes Digital Highway Signs to Hacker Attacks." Security Week, June 6, 2014. Available: http://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks

25 Krebs, Brian. "They Hack Because They Can." Krebs on Security, June 5, 2014. Available: http://krebsonsecurity.com/2014/06/they-hack-because-they-can/

26 Smart America Project. Available: http://smartamerica.org/

acknowledge the intrusion and noted that South Houston is likely not the only vulnerable municipality.[27,28,29]

27 Mills, Elinor. "Hacker Says He Broke Into Texas Water Plant, Others." Cnet, November 18, 2011. Available: http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others

28 Wisniewski, Chester. "Interview with SCADA hacker pr0f about the state of infrastructure security." Naked Security, November 22, 2011. Available: http://nakedsecurity.sophos.com/2011/11/22/interview-with-scada-hacker-pr0f-about-the-state-of-infrastructure-security/

29 Mills, Elinor. "Hacker Says He Broke Into Texas Water Plant, Others." Cnet, November 18, 2011. Available: http://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others /