THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on Cloud Computing

May 15, 2012

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Cloud computing is a paradigm shift in technology that changes the way applications, data and processes are performed, stored and shared. As with any technology paradigm shift, issues such as how the new technologies are used, security, policy, and oversight must be considered when weighing the benefits of adopting the new paradigm. Accordingly, as the federal government executes its Cloud First policy, implications for national security and emergency preparedness (NS/EP) must be considered as they relate to cloud computing plans and programs. Toward these ends, and in the context of a charge to examine cloud computing, two questions were posed to the President's National Security and Telecommunications Advisory Committee (NSTAC) by the Executive Office of the President (EOP):

- **Within the context of NS/EP, what equities should the Government consider moving to the cloud, and in what priority order, if appropriate? What are the sorting/defining NS/EP considerations to determine applicability and value for migration of any given equity to a cloud computing environment?**
- **For equities that do migrate to the cloud, should the requirements for providers supporting NS/EP standards and capabilities differ from the requirements established for commercial cloud providers in general? If so, how?**

The central issue at the core of these questions is: Can NS/EP processes be migrated to the cloud without undue risk? In order to confidently answer the question favorably, the NSTAC recommends that a regime of policy, legal authorities, security and oversight that is comparably-rigorous, complete and trustworthy relative to that now in place for NS/EP activities via legacy means be adopted.

This in turn required the NSTAC to examine several aspects of the described framework as it applies or could be extended to cloud computing. In that regard, the NSTAC studied:

- Policy and legal frameworks: Both have important gaps, and recommended fixes are identified;

- Means by which NS/EP cloud activities, contracts and programs could be identified for specific treatment inside the much larger federal cloud enterprise – An approach based on mandatory service-level agreements (SLA) was developed in detail, and is recommended;

- Security considerations for cloud computing: The NSTAC developed an approach tailored to specific characteristics and priorities of cloud computing, and then designed controls to mitigate identified risks; and

- Priority-access process to support emergency needs: Programs in this area need to be developed, and the NSTAC recommends what to do and how to proceed.

This analysis permitted the NSTAC to conclude that while not in place today, the needed 'comparable' NS/EP-support regime of policy, legal, security and other considerations can be

both defined and implemented. In that context, and conditioned on the availability of such processes, the NSTAC was able to directly address the questions posed.

Within the context of NS/EP, what equities should the Government consider moving to the cloud, and in what priority order, if appropriate? What are the sorting/defining NS/EP considerations to determine applicability and value for migration of any given equity to a cloud computing environment? Conceivably any NS/EP process, including the most sensitive matters, could be moved to "some kind of" cloud, given proper attention to architectural and security decisions. The key qualifier in this judgment relates to the choice of deployment and service model, each seen in the context of the specific mission to be migrated. To support this analysis, the NSTAC deconstructed NS/EP to the mission-function level and subjected each such mission to risk-benefit analysis via a process using NS/EP-specific attributes developed by the NSTAC for this purpose. The NSTAC was able to rank and prioritize recommended progression to the cloud based on the variable benefit of doing so, mission by mission. The result of this effort was a graphical plot of relative value of cloud migration, with some missions appearing more attractive than others, but all being acceptable at some level. Details of this analysis and tables of findings and conclusions may be found in the body of the report.

For equities that do migrate to the cloud, should the requirements for providers supporting NS/EP standards and capabilities differ from the requirements established for commercial cloud providers in general? If so, how? The NSTAC has developed recommendations that address this issue in two parts. First, a list of specific security and related functionalities are identified that should be codified in standard SLAs, using the NS/EP SLAs in the Networx contract vehicle as a point of departure. These should be made mandatory as part of any NS/EP cloud computing contract awarded to any service provider. Second, the NSTAC carefully reviewed existing security-control frameworks from numerous sources, reflecting various points of view and key aspects of domain knowledge and experience of their drafters. From these the NSTAC selected best practices of the federal cloud policy and technology authorities, the cloud computing industry, the audit community and leading international organizations. These were blended into a common language and format, and then distilled into a single, comprehensive and coherent set of cloud security controls tailored for NS/EP attributes and priorities. The NSTAC recommends that these controls become mandatory for daily use in all NS/EP cloud computing implementations.

In the course of implementing the program described here, the most important recommendations included in the report are that the President:

- Direct the appropriate Government organization to develop processes and maintain priorities as described in the body of the report for migration of NS/EP missions to cloud based environments.
- Direct the adoption of NS/EP SLAs in all contracts pertaining to NS/EP cloud computing, which address the following functionalities:
  - Mission emphasis on continuous availability, assured capacity;
  - Identity management (authentication & authorization) for specified mission functions;
  - Periodic third-party audit;

  - Provisions for continuous monitoring;
  - Data encryption in hosted data center (data at rest);
  - Security process transparency for users (EP systems only); and
  - Certification and accreditation (C&A) of hosting systems/processes.
  - For certain national security systems, additional requirements include:
    - Data tagging; and
    - Security management conducted by government service provider.
- Direct the National Communications System (NCS) to adopt cloud security controls developed by this study and found at Appendix E as a comprehensive NS/EP cloud security program, making their use mandatory by NS/EP service owners and auditable by third parties.
- Broaden the definitional scope of NS/EP, as reflected in current law and federal regulation, to embrace information services, as defined, in order to permit the technical nature of cloud computing to fit within the NS/EP definition.
- Direct the expansion of scope of the Federal Risk and Authorization Management Program (FedRAMP) to embrace those governmental information systems reportable under the Federal Information Security Management Act (FISMA) at Federal Information Processing Standard (FIPS) 199 High Impact level, thereby closing a current gap in oversight of a large number of systems relevant to NS/EP.
- Direct the initiation of a Federal program, in collaboration with relevant industry partners, to develop a system for priority access to cloud-based equities in times of need, based on infrastructure degradation due to natural or man-made causes.

Additional recommendations are made in this report in areas of Strategy, Policy and Structure; Security; and Technology.

1.0 INTRODUCTION

Cloud computing is a rapidly-emerging set of technology systems and business processes related to information dissemination, storage and analysis. Definitions and terms related to cloud computing and the specific questions posed to the President's National Security Telecommunications Advisory Committee (NSTAC) by the Executive Office of the President (EOP) are summarized later in this section.

At the core of the task is a foundational question from which all else devolves: Can the cloud be entrusted with critical information processes related to the conduct of national security and emergency preparedness (NS/EP)?

At the highest level of summarization, the NSTAC's response is that if and when cloud computing can demonstrate a regime of policy, legal authority, security, and oversight that is comparably-rigorous, complete, and trustworthy relative to those currently in place for NS/EP activities via legacy means, then the response is "yes." In so doing, efforts must focus on implementing recommendations designed to permit cloud computing to operate at that level in regard to NS/EP.

It is understood that in exigent circumstances in the short term, local authorities may choose to adopt cloud-based processes in the course of their response to emergency situations. That said, the NSTAC believes that it is important to pursue the strategic goal of embracing all of NS/EP within the program recommended in this report.

Fundamental requirements of NS/EP include a high degree of assured availability under any condition of stress; high measures of system and content integrity; confidentiality as required by specific missions; and mechanisms for priority access to resources in the performance of NS/EP functions.

The essential focus of this report is understanding how cloud computing meets those requirements; how the nature of cloud computing causes them to be achieved differently in some cases, relative to legacy systems; and what NS/EP service owners can and should do as a result.

1.1 Charge

In early 2011, the EOP asked the NSTAC to examine the NS/EP implications of the Government's use of cloud computing. In February 2011, the NSTAC Designated Federal Official (DFO) established a Cloud Computing Scoping Subcommittee (CCSS) to examine the issue and present it to the NSTAC for consideration. The CCSS work resulted in the development of the *Cloud Computing Scoping Document*, which was presented to the NSTAC members at the June 2011 NSTAC Meeting.[1] The NSTAC approved the document and moved

[1] See Appendix H for additional information on the CCSS' findings.

to request that the NSTAC DFO appoint a Cloud Computing Subcommittee to further examine the issues identified by the CCSS.

During its examination, the NSTAC members and Government stakeholders raised several questions regarding the Government's transition of NS/EP equities to cloud computing environments. The focusing questions, posed by the EOP, were:

- **Within the context of NS/EP, what equities should the Government consider moving to the cloud, and in what priority order, if appropriate? What are the sorting/defining NS/EP considerations to determine applicability and value for migration of any given equity to a cloud computing environment?**
- **For equities that do migrate to the cloud, should the requirements for providers supporting NS/EP standards and capabilities differ from the requirements established for commercial cloud providers in general? If so, how?**

1.2 Cloud Computing Overview

Cloud computing, the long-held vision of computing-as-a-utility, has the potential to transform the way organizations leverage information technology (IT).[2] New, innovative Web services no longer require large capital investments to support IT infrastructure or substantial recurring operating expenses.[3] Currently, many commercial entities are adopting or considering adoption of cloud computing to improve resource utilization, accelerate service deployment, substantially reduce the cost of IT operations, and deploy new, innovative services.[4] Similarly, for the Federal Government, cloud computing holds the potential to deliver public value by increasing operating efficiency and being more responsive to constituent needs.[5] Commercial migration to cloud computing may occur in direct support of Federal programs, but in most cases, migration will occur for commercial purposes regardless of Federal programs. In June 2011, market research firm Gartner, Inc., estimated that the U.S. cloud market was $44.7 billion in 2010 and is expected to grow to over $100 billion by 2015.[6]

Cloud computing is IT offered as a service by a vendor, rather than infrastructure and applications that are built and maintained by an organization, which greatly reduces or even eliminates the need for an organization to build and maintain its own IT infrastructure. By leveraging shared infrastructure and software applications services, cloud computing allows an organization to build new IT solutions and offer new services more quickly and cost-effectively than building it themselves. It provides elastic resources that enable application services to dynamically scale-up or scale-down based on the user demand. Its computing-as-a utility model enables users to pay only for the resources they actually use. This elasticity of resources, without

[2] Armbrust, Michael et al. *Above the Clouds: A Berkley View of Cloud Computing, UC Berkley Technical Report No. UCB/EECS-2009-28*, February 2009.
[3] Ibid.
[4] "Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2010-1015, 2011 Update", Gartner, Inc, Publication G00213892, June 29, 2011
[5] Ibid.
[6] Ibid.

associated financial premium for this flexibility, has the potential to lower the cost of providing information technology and increase the speed in which technology is made available to consumers.[7]

Despite these benefits, there are uncertainties related to the security and resiliency of cloud-based services.[8] The potential drawbacks are different than those for other IT systems in that existing plans, policies, and practices were established prior to the large-scale introduction of cloud computing in government and potential NS/EP applications. The challenge that many commercial and Government organizations face is in understanding and weighing cloud computing's risks and advantages relative to existing legacy systems. The NSTAC's goal is to arrive at sound policy for use of cloud computing in critical areas related to NS/EP.

The Federal Government's current IT environment is characterized by low asset utilization, a fragmented demand for resources, duplicative systems, environments that are difficult to manage, and long procurement lead times.[9] A service-based architecture, cloud computing has the potential to address these inefficiencies and improve Government service delivery. In December 2010, the Federal Government established a requirement that, to the extent possible, Federal agencies should migrate existing IT services to cloud computing services. The strategy for this Federal migration, the *Federal Cloud Computing Strategy*, was published by the U.S. Chief Information Officer (CIO) in February 2011 to help agencies grappling with the need to provide highly reliable, innovative services quickly despite resource constraints.[10]

In addition to the U.S. CIO's recommendations, several Federal departments and agencies have become involved in advancing cloud computing, with equities ranging from developing cloud standards to transitioning to cloud computing services. The National Institute of Standards and Technology (NIST) has the lead role in developing cloud computing definitions, identifying key areas of interest, and creating a roadmap for technology standards adoption. Additionally, the General Services Administration (GSA) leads the Government's efforts to educate departments and agencies about cloud computing and the Office of Management and Budget (OMB) is developing policies regarding acquiring cloud technology. As part of this effort, GSA, by direction of the Federal CIO Council, established the Federal Risk and Authorization Management Program (FedRAMP) to provide a standard approach to assessing and authorizing cloud computing services. Finally, through the Federal CIO Council, virtually every Federal agency has been involved in some facet of cloud computing policy and strategy.

Cloud adoption by both Government and industry is expected to accelerate rapidly in the near future; however, cloud computing is a relatively new paradigm that has not been extensively studied from an NS/EP risk perspective. To that extent, planned migrations to cloud computing should evaluate the risks to critical NS/EP processes and their impact on both Government and the private sector.

---

[7] Armbrust, Michael et al. Above the Clouds: *A Berkley View of Cloud Computing, UC Berkley Technical Report No. UCB/EECS-2009-28*, February 2009.
[8] Executive Office of the President, *Federal Cloud Computing Strategy*, February 2011. www.cio.gov/documents/federal-cloud-computing-strategy.pdf
[9] Ibid.
[10] Ibid.

1.3.1 What is Cloud Computing?

NIST defines cloud computing as:

"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."[11]

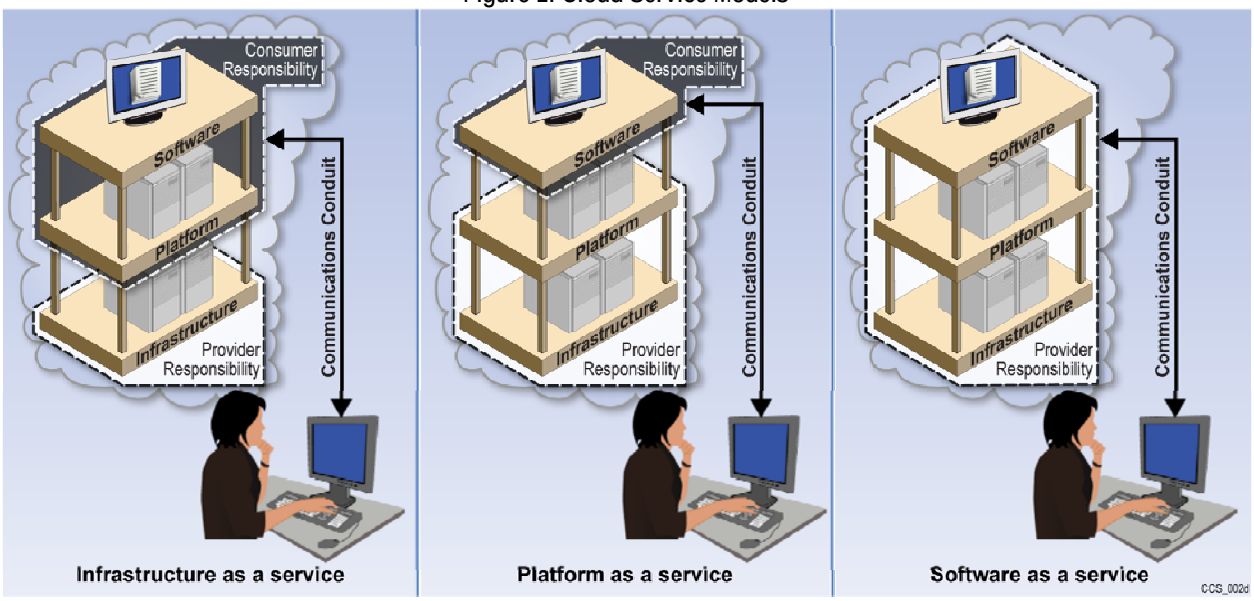
This model promotes availability and is composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[12]

There are three categories of services that are available from a cloud provider: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), depicted in **Figure 1**. NIST defines the service models as follows:[13]

- **SaaS:** The capability provided to the consumer is to use the provider's application running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- **PaaS:** The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
- **IaaS:** The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

[11] *A NIST Definition of Cloud Computing (NIST SP 800-145).* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf
[12] See *Glossary* for definitions.
[13] *A NIST Definition of Cloud Computing (NIST SP 800-145).* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Figure 1: Cloud Service Models

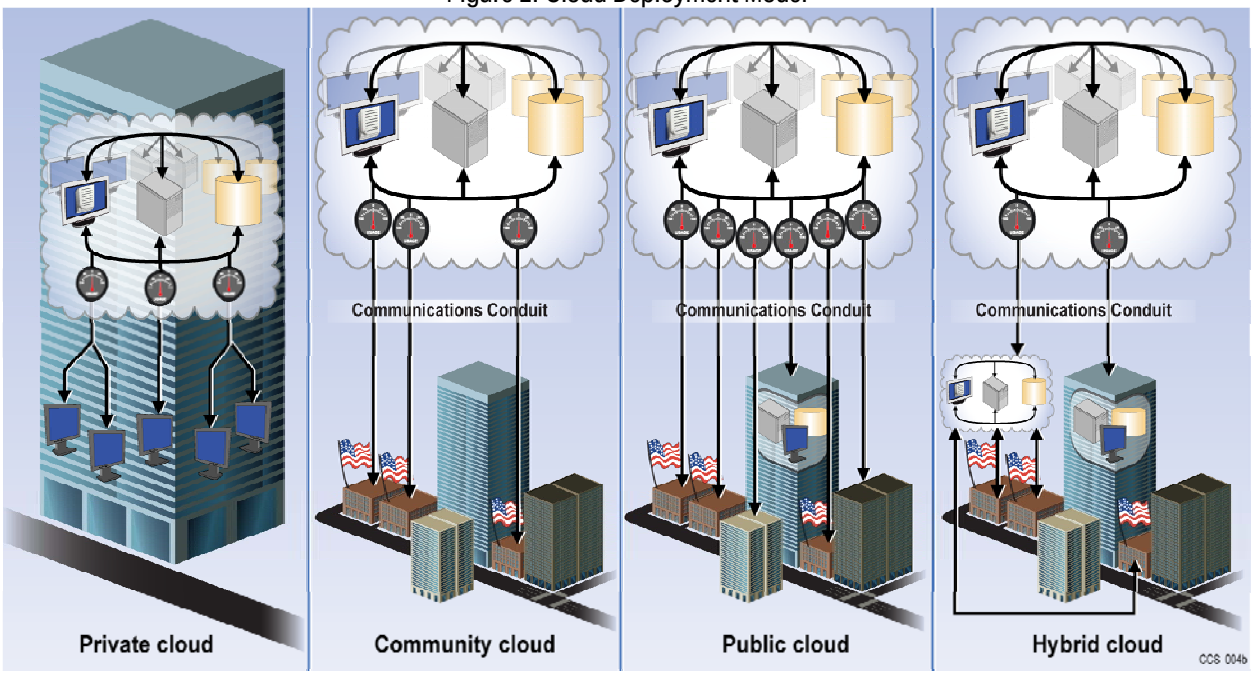


Cloud computing also has four deployment models, each of which provides distinct trade-offs for agencies that are migrating applications to a cloud environment. NIST defines the cloud deployment models, depicted in **Figure 2**, as follows:[14]

- **Private cloud**: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.
- **Community cloud:** The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.
- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.
- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability.

[14] *A NIST Definition of Cloud Computing (NIST SP 800-145).* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Figure 2: Cloud Deployment Model



As the Federal Government migrates some of its applications and data to a cloud environment, it is important for Federal consumers to approach cloud computing as procuring an IT service, not an IT infrastructure, and to focus on new and innovative ways to deliver those services to their consumers. In this paradigm, a Federal CIO or IT program manager has 12 possible methods in which to procure cloud services, depicted by **Table 1**.

Table 1: Examples of Service Consumption in Cloud Computing

Services / Deployment	SaaS	PaaS	IaaS
Private	Agency operation of a software application with chargeback to operating divisions	Agency development of a common environment for multiple development efforts	Enterprise data centers operated by an agency with chargeback to operating divisions on usage
Community	Operation of a travel system for multiple agencies	Operation of a shared software development platform for multiple agencies	Use of common infrastructure for a community of agencies
Public	Providing email from a cloud service provider in a public cloud; the systems that provide the email are the same as those provided to the general public	Operation of a shared software development environment for both public and government developers	Use of a cloud service provider to host agency Web sites
Hybrid	Hybrid is a mix of any of the above deployments and services. For example, an agency might provide public cloud email that has ties to other applications operated in a community cloud infrastructure		

1.3.2 Cloud Technology Adoption

The largest component of the cloud market is SaaS, which was estimated to be approximately 70 percent of market in 2011.[15] The next largest aggregate component of cloud technology is IaaS, which is estimated to be approximately 28 percent of the cloud market.[16] The migration to IaaS will emerge further as organizations augment their existing IT infrastructure with infrastructure provided by cloud service providers (CSP). The smallest cloud offering is PaaS, which is only estimated to be a few percent of the overall cloud market. Organizations will find it cheaper and faster to develop software on a common platform hosted by a CSP, rather than through multiple internal development areas.[17]

The levels of maturity for specific cloud computing technologies vary. SaaS is maturing rapidly and should have broad deployment in applications such as Email as a Service by 2013. Early adopters of cloud email include academic institutions, State and local governments, and Federal agencies, including GSA and the U.S. Department of Agriculture. Furthermore, PaaS, like Web-hosting, is becoming more common; this has been primarily driven by small- and medium-size businesses that do not have the IT resources or capital to host their own Web sites. Government adoption of PaaS will likely increase over the coming years. Early adopters of cloud Web-hosting in Government include the Recovery and Transparency Board as well as the Consumer Financial Protection Bureau. Finally, some agencies have built PaaS models, such as forge.mil, which is designed to improve the speed of software development and sharing among Department of Defense organizations.[18]

Other aspects of cloud computing are still maturing, including the concept of elasticity. Although consumers may believe they have the ability to scale up in an unlimited fashion, there are limits to how quickly cloud providers can scale applications and how much capacity is available.[19]

1.3.3 Cloud Computing Security

There is often an emphasis on the perceived cost and performance benefits of public cloud computing, which tends to overshadow some of the fundamental security and privacy concerns organizations and Federal agencies have with cloud computing environments. As previously noted, many of the features that make cloud computing attractive can be at odds with traditional security models and controls. Several pieces of technology that are critical to successful cloud computing deployments, such as a solution for federated trust, are not yet fully developed. Determining the security of conjoined complex computer systems is also a long-standing security issue that plagues large-scale computing, particularly cloud computing. Attaining high assurance qualities in computing implementations has been the goal of computer security researchers and

[15] *2011 Cloud Computing Planning Guide: The Shift to Hybrid IT*, Gartner, Inc., Publication G00210316, March 15, 2011
[16] Ibid.
[17] Ibid.
[18] Organizations include the Department of Defense and departments within the National Aeronautics and Space Administration.
[19] NIST SP 800-146, Page 4-14, Elasticity: illusion of unlimited resource availability (public).

practitioners, including for cloud computing. Because the design of a cloud service may have NS/EP considerations, it may be required to customize services with the CSP to ensure all service owner needs are met, especially for NS/EP-related applications or data.[20]

Under the *E-Government Act of 2002*, U.S. Government agencies are required to certify and accredit information systems as a standard means of implementing and measuring information security across Government agencies.[21] This process, however, cannot readily be applied to the cloud computing model. As previously noted, OMB established FedRAMP to address this issue and provide a standard approach to assessing and authorizing cloud computing services and products. FedRAMP will also enable multiple agencies gain the benefit and insight of the FedRAMP's authorization, including access to service provider's security documentation packages.

A more detailed discussion of cloud computing security as it pertains to NS/EP specifically is found at section 2.4.

1.3.4 Reliability and Availability of Cloud Services

Typical cloud configurations consist of infrastructure in a data center (e.g., servers, storage and operating systems), applications that are accessed in the cloud (e.g., travel systems used by employees), or specific applications for software development (e.g., forge.mil). The infrastructure or applications are accessed via a networked infrastructure by an end point, which could include desktops, laptops, tablets, or mobile devices, detailed in **Figure 3**. In addition, reliability and resiliency become key characteristics of cloud computing scenarios. If access to either the network, infrastructure, software, or platform is inhibited, then the utility of cloud computing is diminished. Unlike telecommunications and network services, the reliability standards for cloud computing are currently less formal and vary depending on service model, deployment model, or CSP.[22]

One notable advantage of cloud computing is that it reduces single points of failure. Data and applications are not held on one computer, server, or network; instead, they are held on a disparate conglomeration of computing resources. The failure of one node of the system does not impact information availability and does not result in downtime for the cloud consumer. When properly designed, cloud computing provides a highly-resilient and available computing environment. This type of highly resilient and available computing environment is essential to the Federal Government's ability to perform its National Essential Functions and each agency's execution of its Primary Mission Essential Functions before, during, and after an emergency.

[20] NIST SP 800-144, Page 7, Service Agreements.
[21] P.L. 107-347, *E-Government Act of 2002*
[22] NIST SP 800-144, Page 9, Resource Availability

Figure 3: Typical Cloud Configuration

Note that **Figure 3** highlights the three basic elements of a cloud computing system, in terms of the ability to accomplish work. These are:

- The cloud, as described above, including the CSPs involved;
- Communications conduits by which a user achieves access to the cloud periphery; and
- End user/terminal device(s), whether fixed or mobile. Special considerations regarding mobile devices in cloud computing will be addressed in section 2.6.

1.3.5 Cloud Evolution

It is difficult to predict future deployment models for new and innovative technologies, such as cloud computing. There are several emerging trends that will likely influence cloud computing deployment in the future:[23]

- **Computing-as-a-Utility:** This will become a prevalent model of IT deployment for a majority of companies and Government organizations. Economies of scale and improvements in reliability, cost structure, security, and the ease of use will likely compel companies and Government organizations to embrace cloud computing solutions.
- **Standards:** While cloud computing standards are critical for future expansion and market adoption, the technology is relatively nascent and accepted standards have not been established. Several industry consortiums are examining different aspects of cloud computing, including the International Standards Organization study group SC38 and NIST's Standards Acceleration to Jumpstart the Adoption of Cloud Computing program.

[23] Rosenberg, J. and Mateos, A. *The Cloud at Your Service*, Manning Publishing, Greenwich, CT 2011

The standards that are ultimately developed to support cloud computing will have a significant impact on its future deployment. This topic is explored in depth in section 2.8.

- **Mobility:** The rapidly expanding mobility landscape will continue to have a major impact on the cloud adoption rate. When an end user device is pervasive, mobile, and has limited storage and capabilities, cloud is the best available solution to provide applications and storage. Today's mobile device users have embraced cloud computing regardless of potential concerns regarding the cloud's security and availability, opting instead for applications that offer appealing features, storage, and responsiveness. The increasing number and sophistication of mobile devices stimulates the growth of cloud solutions necessary to support them.
- **Open Source Software:** Some cloud implementations rely on open source software for a variety of reasons. This is most applicable to IaaS cloud offerings. The rapid development of cloud technology stimulates open source development by providing an attractive development and testing environment.
- **Industry Considerations:** Given that cloud computing is an emerging IT offering, its associated technologies, prices, and suppliers may change dramatically in the future. As cloud technology matures, demand for the service may increase while prices erode and suppliers emerge and consolidate.

2.0 DISCUSSION

In the course of pursuing the goals outlined above, it is necessary to dissect both NS/EP and cloud computing in ways that illuminate aspects of the questions at the focus of this report. This section will examine the following topics:

- **Policy:** Foundational issues related to legal definitions and organizational charters to help establish the roles, missions, responsibilities, and authorities of major actors in cloud computing for NS/EP.
- **Scoping:** Mapping NS/EP issues and interests within the much larger subject of cloud computing and also cloud computing within and across the entire Federal Government.
- **Security:** The epicenter of NS/EP, the examination of how cloud computing effects historic understandings, practices and processes in this area; also, an examination of security controls designed to mitigate these risk through use of measurable controls.
- **Identity Assurance:** Both authenticated NS/EP cloud access and authorization to conduct cloud-based NS/EP activities.
- **End-User Terminal Devices**: Their role as a component of the NS/EP cloud architecture, considering security and identity factors related to their use.
- **Priority Services:** Development of a classic NS/EP priority-access feature in cloud service and a discussion of provisions for cloud service owners to engage assured, higher-priority cloud use.

- **Standards and Technology:** Their role facilitating secure and interoperable cloud-based NS/EP processes.

The list of topics discussed in this section will implicate three major issues that the Government has focused on significantly and in some cases addressed in law. Since each of these topics predates the advent of cloud computing, current Federal strategies for cybersecurity, identity assurance, and privacy should be reexamined to evaluate cloud computing's effect on them.

- **Security:** Responsibilities for cybersecurity exist in several places across the Government. An integrated, concerted, and sustained security effort must be part of any successful cloud deployment. Given the relationship between CSPs and their consumers, the specific security responsibilities and authorities of each entity must be clearly established.
- **Identity/Access Management:** In 2011, the Federal Government launched a significant effort to address online identity management security through the National Strategy for Trusted Identities in Cyberspace (NSTIC).[24] The NSTAC has long applauded the NSTIC initiative.[25] NSTIC implementation managers should examine that strategy's relevance to cloud computing, as cloud applications are wholly dependent on the ability of cloud users to successfully and securely authenticate themselves for authorized access in a cloud context.
- **Privacy:** As new technologies emerge, the Government routinely examines their effects on consumer privacy. As a result, the Government has implemented various policies and oversight activities in an attempt to protect privacy. The Government should engage in a similar examination for cloud computing. The Administration's February 2012 white paper, Consumer Data Privacy in a Networked World, is relevant to NS/EP considerations in that it reflects a current viewpoint regarding Government's stance on personal privacy.[26]

2.1 High-Level Policy Issues in NS/EP Cloud Computing

2.1.1 Definitions

In analyzing the NS/EP implications of migrating Government data and information to the cloud, the NSTAC studied the definition of NS/EP in the 2010 Code of Federal Regulations (CFR), 47 CFR § 201.2[g], and determined that it should be updated to reflect the current technology landscape. The NSTAC believes that while the 2010 definition is authoritative, it does not take into account newer technology and information services like cloud computing. The current definition of NS/EP services set forth in 47C.F.R. § 201.2[g] is:

"[NS/EP] telecommunications services, or NS/EP services, means those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event

[24] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf
[25] Ibid.
[26] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States."

The term telecommunications is further defined in 47C.F.R § 201.2[k] as:

"[A]ny transmission, emission, or reception of signs, signals, writing, images, graphics, and sounds or intelligence of any nature by wire, radio, optical or other electronic means."

The language here, while appropriate to the scope of legacy NS/EP systems and processes, is too narrow for NS/EP in cloud computing in that it is limited to telecommunications processes and excludes data and applications in storage within the cloud system (commonly referred to as data at rest). Cloud computing is not a telecommunication service in that it does not provide the actual transit mechanism for the delivery of data. It relies on the basic telecommunications infrastructure to connect users to vast computing power, collaboration tools, and data. Future NS/EP mission performance may draw upon information services such as cloud computing services, short messaging, texting, social media in any of several formats, instant messaging and e-mail.[27]

The Communications Act of 1934, amended, contains the following definition in 47 U.S.C. Sections 153 (24):

***"Information service:** The term 'information service' means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service."*

This language embraces not only the immediate issue of data at rest in cloud computing but also many reasonably-foreseeable future advances in technology and refinements in process or procedure by NS/EP-user organizations. Accordingly, in defining NS/EP in the modern technology environment, the NSTAC believes that it would be appropriate to expand the current definition of NS/EP as set forth in Title 47, § 201.2[g] to embrace information services, as defined above.

Of note, the definition of cloud computing in NIST Special Publication (SP) 800-145, *The NIST Definition of Cloud Computing (Draft)*, which was submitted to the Organization for International Standards for consideration as an international standard, reads:

"Cloud computing is 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

[27] 47 U.S.C. 153 (20).

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"[28]

The NSTAC holds that this language supports the definitional analysis in this section, and that it adequately addresses NS/EP in cloud computing by accounting for the evolution of technology, scope, and practice of NS/EP-relevant processes.

2.1.2 Jurisdictional Considerations

Cloud computing presents special complications in the conduct of NS/EP, related to underlying jurisdictions when and where NS/EP services are hosted. As noted in section 1.3, a basic characteristic of cloud computing is the tendency for cloud-hosted data, applications, and services to be housed in architectures and servers in disparate locations. In so doing, NS/EP-related data and services may become subject to unique legal and policy frameworks in the hosting jurisdictions. While it is in the interest of NS/EP that services, cloud-based or otherwise, be available, predictable and consistent as required by the mission, those attributes cannot be guaranteed under current jurisdictional variances related to cloud computing.

From an NS/EP standpoint, this situation presents itself in three dimensions:

- U.S. statutes and regulations related to the conduct of international commerce;
- Foreign legal and policy regimes that apply in the case of U.S.-originated NS/EP equities located in their jurisdictions; and
- Differences between legal and regulatory codes of U.S. States and territories.

In the international cases above, the topic is further impacted by several issues:

- Cloud services may be subject to the International Traffic in Arms Regulations (ITAR), which controls the export and import of defense-related articles and services on the United States Munitions List. ITAR does not apply to: (1) information related to general scientific, mathematic, or engineering principles commonly taught in schools and colleges or information that is legitimately in the public domain; (2) general marketing information; or (3) basic system descriptions. As every Government agency and company within the ITAR regulation scheme are bound to comply with its provisions, the cloud must also be compliant. Further, owners of cloud-based content that has data subject to the control of ITAR/Export Administration Requirements, the Health Insurance Portability and Accountability Act, or the Office of Foreign Access Control must be compliant with the regulations.
- Other specific/relevant statutes include the Export Administration Act, the Arms Export Control Act, and the Trading with the Enemy Act, implemented and enforced by the Department of Commerce, Department of State, and Department of the Treasury, respectively. Software code, data, and systems are included in the definition of exports, for the purposes of these statutes.

[28] NIST SP 800-145 for the full definition including descriptions of the five essential characteristics, three service models, and four deployment models.

- Laws and regulations differ across nations. The European Union, for example, has stringent requirements for privacy and data protection and retention that are not found in non-European Union nations. Neither the NS/EP definitions nor the Communications Act of 1934, amended, addresses concerns about data at rest located in a foreign country.

Although U.S. NS/EP service owners may dictate the jurisdiction when initially deploying cloud-based NS/EP solutions, each jurisdiction may have statutes and regulations that treat cloud services differently. For example, some cloud service providers avoid providing service in certain state jurisdictions which levy taxes on online transactions.[29]

Given the event-generated nature of many NS/EP mission responses, it is often impractical for NS/EP service owners to try to limit the jurisdictions in which their content may be hosted. In some deployments, this may be an attractive option during the contract-negotiation phase. It is far more likely, however, that sponsors of relatively-sensitive national security-related data sets and applications will seek to mandate and control the geographic and jurisdictional scope of cloud-based equities. Therefore, it is important that when considering moving services to the cloud, the NS/EP service owners must take care to review all applicable laws and regulations to ensure that the NS/EP service can be effectively available in each of the jurisdictions where it might be operationally needed, and to contractually restrict storage if and where made necessary by the nature of the mission and associated data and processes.

2.1.3 Contracting for NS/EP Cloud Services

The definitional discussion in section 2.1.1 has a cascading effect on processes for procuring NS/EP services, in that the definitions set forth in the *Communications Act of 1934*, as amended, and in the CFRs are applicable to traditional common carriers, but not to all potential CSPs.

Multiple existing acquisition vehicles are available for the procurement of cloud services. These include Multiple Award Schedules, Government Wide Acquisition Contracts, and multi-agency Indefinite Delivery/Indefinite Quantity contract. However, the terms and conditions that account for NS/EP functions are not standardized or universally incorporated into the base contract. That means that the unique requirements for NS/EP must be inserted in individual agency task orders. In comparing a traditional telecommunications acquisition, like GSA's Networx, with other acquisition vehicles, Networx has outlined standardized requirements for NS/EP, while, in most cases, the other vehicles have not. This means there is risk that individual agencies may incorporate NS/EP terms and conditions that do not meet the requirements.

Consistent with the case made above, regarding extension of classic NS/EP definitions and processes to embrace an expanded scope if and when NS/EP processes migrate to a cloud-based environment, the NSTAC recommends that NS/EP cloud services only be accessible via contracts including the same security and other provisions as those in place for NS/EP services delivered via legacy means. The NSTAC also proposes that the President direct the OMB to develop common service level agreements (SLA) for NS/EP-in-the-cloud and to issue a policy

[29] http://www.theitservicessite.com/author.asp?section_id=1577&doc_id=236085

directive requiring all Federal agencies procuring information services involving NS/EP-in-the-cloud use these standardized SLAs. Specific content for these SLA's will be discussed in section 3.2.

2.2 Policy Relationships and Adjacencies

The role of policy-based solutions to support cloud migration cannot be overstated. It is widely understood that policy often lags technical innovation and invention. Consequently, a number of concerns regarding cloud computing are necessarily addressed via organization and policy authorities, vice technology fixes. Wisely-crafted policies can be enablers and levelers, permitting technical measures to work predictably and efficiently.

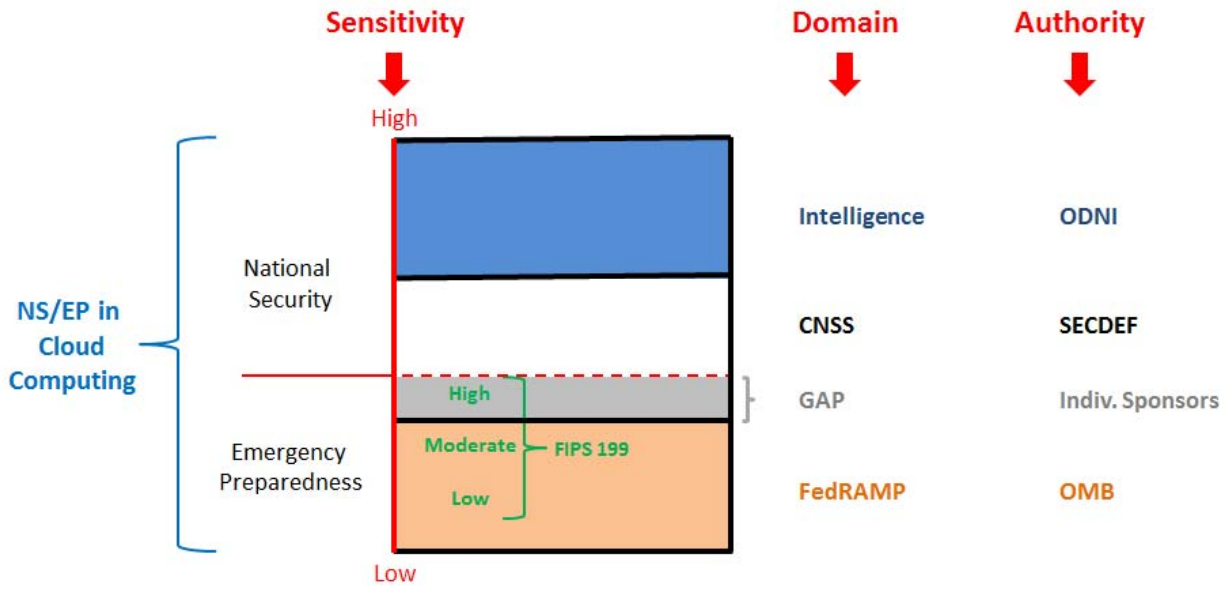
In addressing Federal cloud computing management specifically, three policy and authority frameworks exist:

- The scope of FedRAMP embraces the security aspects of cloud computing systems reportable under the Federal Information Systems Management Act (FISMA) at levels of "low" and "moderate" risk impact level, as defined by Federal Information Processing Standard (FIPS) 199.[30] In Fiscal Year 2009, these comprised 88 percent of the Federal systems reportable under FISMA.[31] The scope of FIPS 199, at any level of sensitivity, excludes "national security systems," as defined in 44 U.S,C 3542.[32]
- The Committee on National Security Systems (CNSS), chaired by the Secretary of Defense, is responsible for overseeing national security systems in accordance with National Security Directive 42 (NSD-42).[33]
- The Office of the Director of National Intelligence (ODNI) has created and manages a cloud implementation process across the intelligence community (IC). These systems lie outside the definitional scope of FIPS 199, but do overlap with the scope of NSD-42.

Despite the large-scale embrace of these three frameworks, a gap remains, bounded by the high end of the current scope of FedRAMP and the low end of the definition of national security systems, per NSD-42, as shown in **Figure 4.** This gap encompasses the 2315 FIPS 199 High Impact systems reportable under FISMA in 2009, or 12 percent of the reportable total number of systems for that year.

[30] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
[31] Office of Management and Budget, *Fiscal Year 2009 Report to the Congress on the Implementation of the Federal Information security Act of 2002*, page 28, table 2, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf
[32] 44 U.S.C. 3542
[33] http://www.fas.org/irp/offdocs/nsd/nsd42.pdf

Figure 4: Federal Cloud Computing Policy Relationships



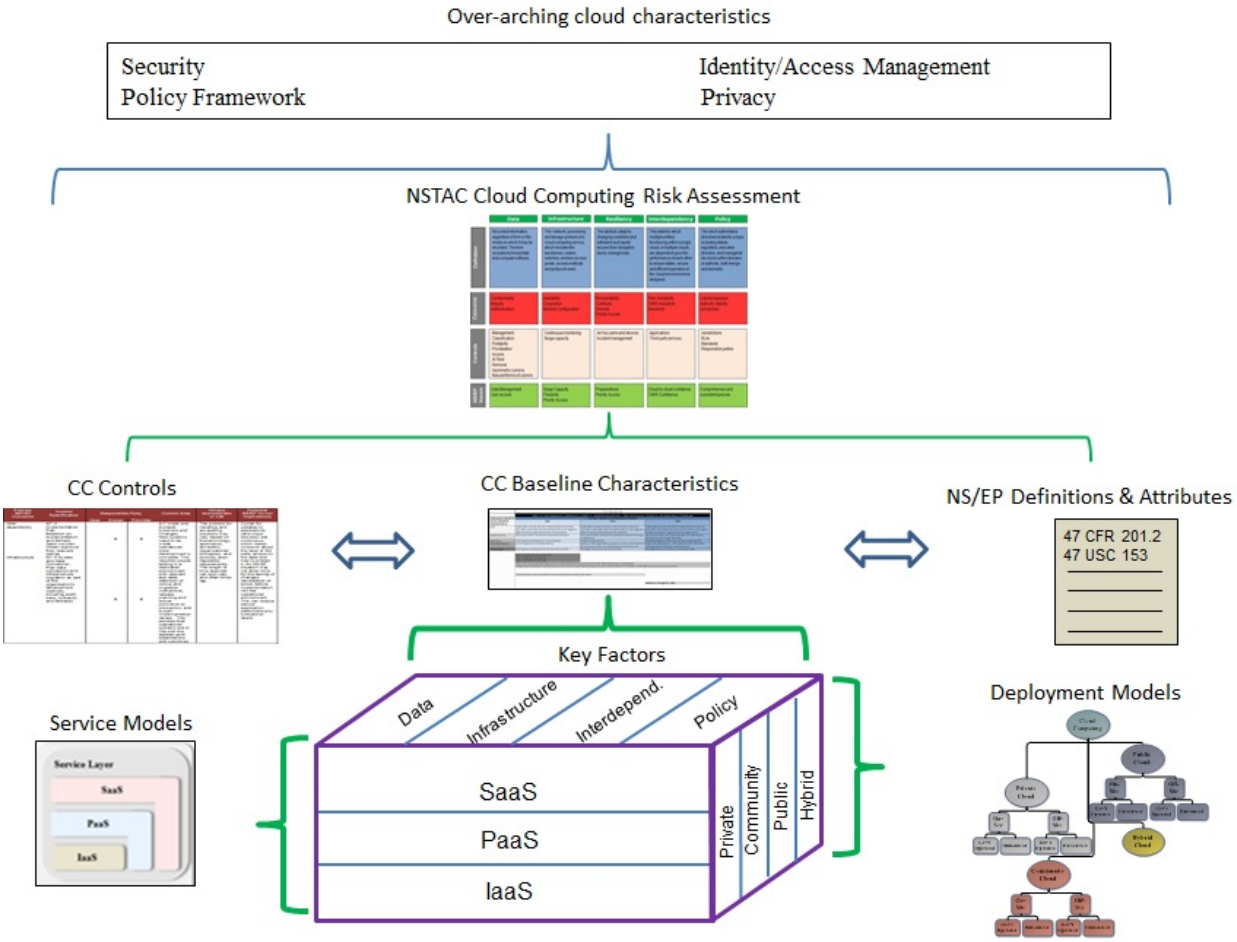
Of the three policy authorities cited here, two are actively seeking to guide and direct cloud implementation at this time; the CNSS has thus far not created specific cloud-management frameworks or policies for those national security systems not within the scope of intelligence community efforts.

2.3 Mapping Cloud Computing in NS/EP Context

It is important to recognize that the charter and scope of the NSTAC's effort is not all of cloud computing or even Federal cloud computing (and critical civil infrastructures). Instead, the limits of scope are those of NS/EP *within* cloud computing. It is therefore necessary to define, map, and understand the intersection of NS/EP and cloud computing within the context of larger domains.

The NSTAC created a map of cloud computing in the context of NS/EP, depicted in **Figure 5**. The map was developed from a basic three-dimensional model embracing defined cloud deployment and service models and a set of features deemed to constitute the critical elements of a cloud system. Starting from that basis, the model builds progressively, leading to a holistic view of cloud computing as it pertains to NS/EP, as summarized in **Figure 6,** Cloud Computing Risk Assessment.

Figure 5: Cloud Computing NS/EP Map

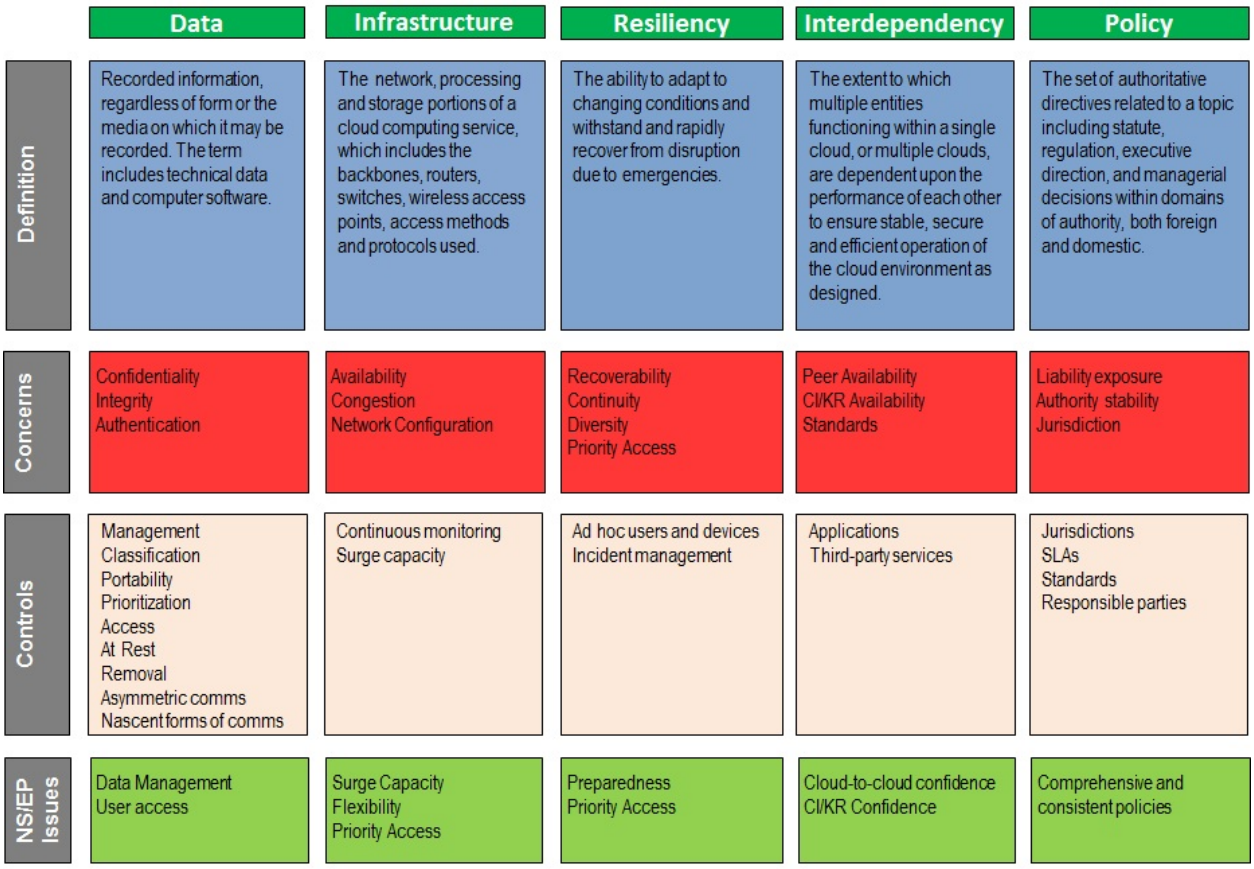


See Appendix D for a detailed discussion of the analytic path from the basic three-dimensional model to the Risk Assessment chart. Recognized security vulnerabilities are defined, categorized, and mitigated by a set of NS/EP cloud computing security controls identified through the report and described in section 2.4.

2.3.7 NSTAC Cloud Computing Risk Assessment

Figure 6 summarizes the NSTAC's cloud computing risk assessment, which was designed to determine whether or not the specific risks and threats can effectively be controlled thereby permitting the key NS/EP considerations to be achieved and maintained. The chart: (1) defines each of the five key cloud factors; (2) identifies concerns related to that aspect of a cloud service: (3) offers controls to reduce those concerns, which are drawn from the controls matrix (Appendix E); and (4) shows the particular NS/EP concerns for each factor.

Figure 6: Cloud Computing Risk Assessment



2.4 Cloud Computing Security

A foundational consideration in NS/EP, security is often cited as an issue of concern in cloud computing. The largest single section in this report due to the complexity and diversity of the topic, the discussion here consists of two major subsections:

Risk Management: Evaluation of potential benefits of cloud computing for NS/EP against the potential security risks of operating in a cloud-based environment. These are studied with emphasis on new or evolved threats in the security/risk domain, resulting in a need for NS/EP managers considering cloud migration to focus on adjusting security strategies and practices to meet those threats. The NSTAC also examined specific risk issues related to cloud deployment models, service models, and other factors.

Security Controls: The NSTAC has identified various best practices of government, industry, auditors, and leading international organizations for cloud computing. The NSTAC distilled these disparate control frameworks into a common format to identify and create a consolidated list of security controls for NS/EP cloud computing.

2.4.1 Risk Management in NS/EP Cloud Computing

While cost avoidance is frequently cited as an incentive to cloud migration, the NSTAC did not analyze cost as a variable in cloud computing migration. The proper approach to cloud computing migration for NS/EP should focus on the mission and not be driven by expectant cost savings. Specifically, Federal agencies should conduct an analysis of new benefits, functionalities, and incremental costs and risk exposures, then compare them to understand the cost versus benefit.[34] In so doing, agencies can identify areas of greater and lesser net value, based on perceived mission benefit as opposed to changed risk exposure, specific to defined NS/EP missions.

One emergent issue in cloud computing cost analysis is that in some cases, end user losses are underwritten by CSPs in return for service adoption.[35] While this approach might have the desired effect of fueling cloud adoption in the general public, it does not address NS/EP concerns regarding data hosting.

When discussing the risks and benefits in cloud computing, it must be noted that although the underlying technology is not new, the business models and applications often are. Thus, cloud computing may be considered an emerging field in commerce and technology. It is generally expected that conditions will evolve over time; the market will cause rationalization and consolidation around agreed standards; business models will be refined as the market becomes more sophisticated and discerning in the service selection; and offerings that fail to deliver value at reasonable risk will be remedied or perish. From the view of contracting service owners, cost savings are expected to normalize, becoming both more predictable and more attractive.

Risk management is the process of comparing benefits to risks to develop policies and processes that identify acceptable risks while still achieving an organization's defined goals. Organizations considering migrating any NS/EP equity from a legacy IT environment into a cloud-based one can directly compare the changes in both positive and negative terms. Within cloud computing, NS/EP represents a special case, with narrowly-drawn missions and defined organizational participation. Valued performance attributes and their relative weights differ for NS/EP cloud deployments; for these reasons, special considerations associated with NS/EP are required to weigh value and risks associated with cloud migration.

As previously stated, advantages of cloud adoption are unique to every situation, organization and deployment, but generally include reduced needs in hardware, facility space, utilities, and human resources as well as expanded functionality, versatility, and interoperability.[36] A recent study of cloud computing users found that the primary reason and benefit for cloud adoption was improved connection of employees using a range of formerly-non-interoperable legacy

[34] See section 3.1 on cloud migration of defined NS/EP mission functions for additional information
[35] This model is similar to that of the consumer credit card industry, which does not guarantee the absence of fraud, but will not hold the end user consumers accountable if it occurs.
[36] Federal Cloud Computing Strategy, White House, February 28, 2011, http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf

systems.[37] This particular capability would be attractive to NS/EP managers in a number of scenarios.

The NSTAC believes that imaginative and creative managers will experience potential rewards in the form of either enhanced or perhaps even completely-new functionality in the approach to their organizations' missions. These insights are expected to emerge with practice and experience, over time. Further, they are likely to only be found and exploited by those who seek to understand that cloud computing is not simply a change in technology but more significantly a force impacting business practices, culture, and even organization.

Security is difficult to measure because its costs are difficult to isolate, especially when extended to potential loss of intellectual property or privacy. IT managers have sought to define levels of needed security based on the nature and content of systems. As previously noted, the management approach to security in cloud computing requires careful attention. Some considerations, threats and mitigation techniques work identically as in legacy environments, but some work differently or are not applicable. The NSTAC finds that security issues related to cloud computing can be collected and examined in four groupings:

1. **Classic Security Issues:** Similar to legacy architectures and systems; many of the cloud computing security concerns can be considered part of this grouping. Many authoritative documents outline practices, procedures, and requirements to protect information relevant to NS/EP.
2. **New Security Issues:** In addition to jurisdictional issues, discussed in section 2.1.2, this category includes security issues created by the technical nature of cloud computing, including:
   - Multi-tenancy: Multi-tenancy is the process of hosting multiple data sets and applications from various sources in a common cloud environment. Service owners hosting materials may have no knowledge of other tenants that have been granted user access to the shared cloud environment. Classic perimeter-based security controls may be neutralized or circumvented for multi-tenant clouds. This risk is far more pronounced in a public cloud, but may exist in any type of cloud.
   - Layered nature of cloud offerings: The layered nature of cloud computing complicates its application to NS/EP equities. For example, it is possible to host data in an IaaS cloud model while also hosting software and applications from a different vendor within the same cloud. In doing so, any possible security weaknesses associated with one vendor may infect the other, as well as their mutual customer. While this risk exists in networked information systems, its potential impact is amplified in a cloud computing environment.
3. **Classic Security Issues Amplified in Cloud Environments:** These security issues appear to be conventional and accounted for in traditional procedure or risk calculation; however, the potential significance is greater in cloud computing, and this new consequence weighting may render risk management efforts unbalanced. These include:

[37] CSC Cloud Usage Index, study by TNS, 2011, pg. 2.

- Corrupted service provider: Potentially more dangerous than the classic insider threat because it presumably has power over a greater scope and expanse of data and processes; by the nature of the cloud, a corrupted service provider can cover its movements almost completely. This potential for error or malice on the part of technical personnel employed by the service provider demands close attention.
- Impact of service provider business default: Service provider default on agreed terms and conditions can be severe in cloud environments. Cloud consumers must be aware of this and plan for this to avoid service disruption caused by lock-in to a service provider who defaults. Ensuring data and service portability is essential for the long term successful use of cloud services.
- Data aggregation: Bits of data, which may be insignificant individually, can be assembled to create sensitive processes or information. The scope of potential data aggregation in the cloud requires managers to consider this factor differently than in legacy systems.
- Data exposure to exploitation: While stored data is always vulnerable to exploitation attacks, it is more easily accessed when stored in certain types of clouds than if protected inside the security domain of its owner, as in most legacy environments. Encryption of cloud-stored data is a basic security requirement for NS/EP.
- Security process management: Legacy system administrators create and manage security regimes appropriate to the data and applications they protect. In so doing, they account for reporting, compliance and other requirements specific to their jurisdiction and system/data content. Special requirements related to security of types of content may be applicable (e.g. personally identifiable information [PII], medical or financial information). Data owners need to be able to examine security processes employed by cloud hosts to ensure that all necessary requirements are being met.
- Forensics: An emerging field within computer security, forensics provides a potential path to attributing threats to attackers, based on detection and analysis of traces left as perpetrators move through architectures and machines. In the cloud virtual machines can be established and shut down rapidly; once deleted, there may be no fingerprints left behind to support forensic analysis.
- Identity compromise: This weakness is focused on the interfaces between device, path, and cloud perimeter. In a cloud environment, these are often more complex and varied than in legacy environments. They also offer more opportunities for a malicious user to leverage compromised access credentials to gain access to and navigate the cloud.
- Weakest-link: There is an understanding in systems security that a network's weakest link offers the easiest access to attackers, thereby permitting circumvention and compromise of some or all network protections, even those guarding stronger net participants. In a cloud environment, the potential for such compromise to occur via interdependency on partnering clouds is more difficult to detect and counter. There is also the related risk of malicious clouds, created for the express purpose of facilitating penetration of other clouds.

4. **Negative Security Consequences of Basic Cloud Attributes:** This category includes risks and security concerns that result directly from positive characteristics of cloud computing.

   - Speed of adoption and hardware development: A basic concept behind cloud computing, whether based upon virtualization or proprietary technology, is the speed of adoption. Having the ability to rapidly move applications into and out of cloud infrastructure allows for flexibility and time-to-market that has not previously been accomplished. It is expected that cloud service providers will keep pace with advancements in both hardware and software to take advantage of new features and functions as they become available. From a security perspective, this may have a negative impact in that speed-to-market can be counter to the goals and schedules of traditional security evaluation. Where the market drives rapid advances in solutions, we may have to modify our strategy for security oversight by incorporating it into programs already in use by the various cloud authorities (identified in section 2.2). This approach underlines the criticality of subjecting all Federal NS/EP cloud migrations to a defined management and policy authority.
   - Software life cycle: The process of software development, testing, and fielding is at odds with the market's increasing demand for fast delivery, availability, and updates. Cloud computing can immediately offer new applications and software to virtually unlimited user communities. In so doing, developers are further constrained to avoid detailed code validation processes, even if required by policy. Use of machine-generated code is rising and may create potential open-ended security holes and vulnerabilities.
   - Multi-domain separation: In controlled IT architectures, it is necessary to embrace multiple levels of security and data sensitivity. Architectures and processes establish safeguards to ensure the users and data can transit domain layers in secure, monitored, and controlled ways. In the cloud, data and applications representing multiple sensitivity levels may coexist in uncontrolled adjacencies. If conducted maliciously, migration across these environments may be uncontrolled or even undetected.
   - Mobile-device capabilities: The ability to manage and manipulate cloud resources dynamically and remotely, including by mobile devices, is advantageous in many scenarios. At the same time, there is a growing risk that attackers could access credentials, giving them broad cloud controls by seizing or otherwise compromising such devices.
   - Cost versus risk tradeoffs: The normal cost differences between NS and EP systems may impact the delivery and adoption of cloud solutions. At the EP end of the continuum, security requirements are less restrictive and therefore the related costs of implementing adequate security in a cloud solution may be significantly offset by the advantages of agility, adaptability, scalability and other cloud benefits. At the other end of the spectrum, NS systems frequently have significant security requirements that require validation and verification or even certification from multiple parties. NS systems are often required to revalidate, verify, or recertify with each configuration change. The much larger costs (both money and time) normally associated with

developing, deploying and certifying cloud based NS systems – as opposed to EP systems – thus may offset the cloud advantages and delay rapid adoption and deployment. This may mean that cloud use is less desirable for some NS related systems. System specific risk/benefit analysis is required to determine the value of employing cloud service for specific systems.

- Concentration of assets: Aggregation of data, applications, and other resources in data centers associated with cloud computing permits managers to achieve a higher density and quality of security oversight. Those same factors cause the collected resources to become lucrative targets for attackers.

The net effect of the foregoing should be to demonstrate that any prospective cloud deployment must carefully consider the total security effort required, and especially its focus. Many of the efforts and expenses associated with security hardware, software, staff, training, processes, procedures, and policies require adaptation to deliver comparable performance for migrated NS/EP equities. These adaptations will require time and dedicated resources. Failure to make these changes could lessen the levels of security necessary. Accordingly, due to the criticality of NS/EP functionality, migration of NS/EP processes to cloud-based environments should only occur under appropriate oversight and policy supervision.

Table 2 outlines some of the variables, both positive and negative, that affect risk management in cloud computing. Each variable may positively or negatively influence any prospective cloud migration decision.

Table 2: Benefits and Risks of Cloud Computing

Benefits	Concomitant Risks
Cost savings	Not automatic or predictable in size; needs to be consciously accounted for in architecture/planning
Potentially positive effect on government/civil NS/EP collaboration	Data ownership/control; interoperability unless common standards are developed/adopted
Information sharing/collaboration; data analytics	Multi-tenancy with potentially malicious users
Access to best practices	Enhanced insider influence
New functionality	Incompatibility of standards; proprietary processes; jurisdiction-based policy conflicts
Elasticity in rapid fielding of new services or applications	Risk of exposure to unvetted, new net participants

2.4.1.1 Risk Management as a Function of Service Model

The division of security responsibilities and authorities varies across cloud service models, though a service provider's role generally increases as one moves from IaaS to PaaS to SaaS. The adoption of specific service models leads directly to an understanding of the residual security responsibilities of data and application service owners. Service owners might find they have a reduced need to account for security of their cloud-hosted processes; however, if service owners retain responsibility for the availability and integrity of those processes, the fact that they may lose visibility into or influence over their protection might be seen as a detriment. As cloud

services continue to develop and evolve, CSPs will likely support extended security protection offerings to help mitigate security risks. Any lack of transparency within these processes may be difficult for users seeking to conduct due-diligence of the security frameworks that protect the mission-critical processes or fulfill requirements based on jurisdiction, the nature of data, or processes involved. As such, NS/EP cloud-hosted processes may require special provisions for visibility into CSP security mechanisms.

2.4.1.2 Risk Management as a Function of Deployment Model

Selecting the proper deployment model is a major consideration when managing risk, as service owners must decide which deployment model to adopt for their mission. Risk generally increases as one moves outward in scope from private to community to public deployment models. This is particularly clear as one moves from any deployment model other than public to any public or hybrid-public cloud. In this environment, cloud services and data are more exposed, with concomitant risks to confidentiality and integrity. As section 3.1 outlines, this is a concern for some NS/EP missions.

Private clouds may be deployed either on-site or off-site. If the private cloud is located off-site or if the service owner's organization spans multiple physical sites and wishes disparate staff to access the same private cloud, it introduces risk to a private cloud's networking availability and security. This occurs because performance dependencies are established to resources that exist off of the service owner's site and are not directly under the service owner's control, and because failure to properly implement and configure any of a number of security-related processes could allow outsiders access.

Private clouds mitigate the risks from multi-tenancy by restricting the number of possible attackers; all of the clients would typically be members of the subscriber organization or authorized guests or partners. The on-site private cloud is, however, still vulnerable to attack conducted by authorized but also malicious insiders.

For public clouds, subscribers typically connect to providers via the public Internet or a similar networked infrastructure. The dependability of connections depends on the Internet or network's infrastructure of Domain Name System servers, the router infrastructure, and the inter-router links. Connection reliability can therefore be affected by misconfiguration or failure of these components as well as network congestion or attack. Additionally, subscribers may require a connection via an Internet service provider.

2.4.1.3 Cloud Security "Seal of Approval"

While experienced and capable security organizations may be well-prepared to protect legacy environments and systems, the special needs of cloud security suggest that, at least initially, there is need for dedicated cloud security services and expert practitioners. One possible approach to address this need could be the creation of a cloud security "seal of approval." Under this concept, highly-skilled security organizations could create criteria designed to validate the skills and abilities of candidate cloud security service providers. Other organizations could test candidate organizations to the defined criteria, after which passing candidates would be managed

within the FedRAMP process and made known to end-user organizations in the form of an approved vendor list.

2.4.1.4 Adversary Action as a Variable in Cloud-Risk Management

Risk management calculus recognizes possible exploitation and attack risks (e.g., identity compromise, data exfiltration). The expectation of direct attack on cloud-based processes varies across NS and EP, and by scenario. For example, it is unlikely that efforts of government, non-governmental organizations, and other responders providing post-natural disaster relief would encounter any significant denial-of-service (DOS) (availability) or data exploitation (confidentiality) attacks, unless such attacks were part of a larger attack scenario. On the other hand, sensitive data and applications stored in clouds would be attractive targets, and as noted, there are a number of cloud characteristics that provide new advantages to such attackers. Section 3.2 outlines procedures currently in place or being developed within the NS community's cloud migration efforts that recognize and seek to respond to these risks.

One of the most detrimental situations would be a response that is precipitated by a large-scale man-made terrorist event. There is some evidence of intentional disruption of emergency-responder communications and coordination mechanisms in such cases. In so doing, efforts to further harm target populations are conducted by the same terrorists that executed the original attacks.[38]

Unfortunately, emergency response organizations and infrastructures cannot selectively provide firefighting, ambulance and similar response services to terror attacks versus other incident types. Any efforts to harden such response capabilities would simultaneously weaken their flexibility, a key attribute in many EP situations and thereby largely defeat the plug-and-play nature of cloud computing. In this regard, the greatest risk posed by deliberate efforts to degrade cloud-based emergency response performance would be seen as attacks on the access to cloud-based services (e.g., DOS/availability attack).

As discussed, cloud security needs and corresponding technological and procedural measures are quite different from those of legacy environments, a reality for which many organizations are not prepared. Cloud migration should only be contemplated by those organizations that have carefully considered and prepared for the changed security environment. Formalized cloud security controls will play a large part in that process.

2.4.2 Cloud Security Controls

An important practice in effective risk management is the implementation, assessment, authorization, and monitoring of a set of security controls that are commensurate with the risk-impact categorization of a given NS/EP mission function. In the current cloud computing environment, there are a number of existing frameworks that identify, categorize, and define

[38] *FDNY Counterterrorism and Risk Management Strategy"*, Page 3. www.nyc.gov/html/fdny/pdf/publications/FDNY_ct_strategy_2011_12.pdf and Rand Corporation *"The Lessons of Mumbai" Page 7.* www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf

important risk principles and security controls to protect the confidentiality, integrity, and availability of data processed and stored in the cloud. These frameworks include:

- Cloud Security Alliance (CSA) *Cloud Controls Matrix;*
- ISACA (formally the Information Systems Audit and Control Association) *IT Control Objective for Cloud Computing: Controls and Assurance in the Cloud;*
- European Network and Information Security Agency (ENISA) *Cloud Computing: Benefits, Risks and Recommendations for Information Security;* and
- FedRAMP Security Controls Baseline.

The NSTAC evaluated these frameworks to identify the key risk factors that NS/EP service owners can consider when migrating NS/EP functions to cloud computing platforms. The NSTAC's evaluation noted that each framework addresses different objectives and offers a set of insights that could be calibrated to assist the evaluation of NS/EP-related cloud services. Although there are distinctions among these approaches, there is considerable alignment among the controls, risks, and/or principles defined. As a result, there is a mutually-reinforcing relationship among the frameworks. For example, FedRAMP provides a set of controls that meet the baseline requirements for Federal agencies operating non-national security systems, CSA's framework provides controls that potential cloud service customers can consider when migrating operations. ISACA's framework, while addressing some of the same controls as CSA, focuses on evaluating compliance factors. Finally, ENISA's study focuses on understanding the broader, holistic view of assessing risks and benefits for cloud services for Government functions. The salient points of the different frameworks are summarized below.

- **Identifying and aligning the range of controls:** The CSA's Cloud Control Matrix provides security control requirements built for the cloud and establishes fundamental security principles for service owners and CSPs. It also serves as a scheme for evaluating the risks related to services delivered by a CSP. The CSA's approach represents an industry-led initiative that intersects with security standards, regulations, and controls.
- **Evaluation and compliance factors:** ISACA's IT Objectives for Cloud Computing focuses on IT governance controls that are customizable for the cloud. This approach recognizes the unique nature of the cloud as a challenge to classic/conventional audit processes and techniques. It also focuses on IT processes– not functions or applications– from the process owners perspective, who principally assumes the responsibility of the IT functions that support and enable the business processes under their purview. Additionally, framing the controls using a life-cycle approach calls attention to the importance of upfront planning, organizing, and coordinating with responsible parties to develop principal and fundamental documents or constructs, such as an agreed-upon taxonomy of service terms and definitions. This framework also provides assurance on the effectiveness, efficiency, compliance, and reliability of the control activities to assess the adequacy of implementation.
- **Understanding holistic risk benefit calculations:** ENISA's Cloud Computing: Benefits, Risks and Recommendations for Information Security identifies policy and

organizational, technical, legal, and other IT risks relevant to the cloud environment from the service owner's perspective. In reviewing the work of a European Union agency, the NSTAC incorporated an international perspective on cloud computing risk considerations that further validated a common set of risks emphasized in the other frameworks.

- **Extending a consistent risk management process to the cloud:** FedRAMP leverages and streamlines the Federal Government's process for assessing and authorizing security risks for cloud-based systems.[39] By adopting a "do once, use many times" approach, FedRAMP seeks to apply a consistent and rigorous mechanism for agencies to apply controls for managing cloud risks for their low and moderate impact systems. FedRAMP extends existing FISMA compliance requirements from the traditional computing environment to cloud computing for applicable low and moderate impact systems and data. When fully implemented, FedRAMP's baseline controls will serve as the minimum benchmark to which Federal agencies and CSPs providing services to Federal agencies must adhere to adequately address the risks associated with migrating services and functions to the cloud.

2.4.2.1 NS/EP Implications

Applying these frameworks to the NS/EP environment revealed that a new risk management approach is required for service owners migrating NS/EP functions to the cloud. This is due to the criticality of the communication needed, the requirement to maintain readiness in all circumstances, and the sensitivity of the data being transmitted. Different cloud deployment and service models present varying levels of risk for any given NS/EP mission function, which increases the complexity of the risk calculus. Though not wholly comprehensive, the following list illustrates a set of NS/EP implications and risks for each of the five key factors— data, infrastructure, resiliency, interdependency, and policy—that are not fully addressed in traditional risk assessment approaches.

Data

- **Management:** Data management presents an imposing challenge when faced with the imperative that the right information needs to get to the right people at the right time. For instance, an NS/EP event can generate vast amounts of data that must be managed effectively to ensure that the correct type and classification of data is reliably disseminated and exchanged and transferred, purged, or stored with the appropriate safeguards, such as encryption. This must be completed while maintaining the confidentiality, integrity, and availability of the information.
- **Classification and portability:** During an NS/EP event, data may need to be rapidly reclassified, requiring commensurate and immediate changes to access controls. This data may then need to be seamlessly ported from one CSP to another or back to a traditional, in-house information system to preserve and/or prevent the destruction of data.

[39] NIST SP 800-37 *Guide for Applying the Risk Management Framework to Federal Information Systems* and the NIST SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*

- **Prioritization and access:** Challenges can also arise in priority processing and priority access to shared resources if there are competing incidents of national significance, such as a natural disaster in the United States or military action abroad.
- **Data at rest:** Loss of data or prolonged inability to access critical data can have significant impact on operations. For instance, if there are requirements to preserve certain types of data (e.g., access logs) for set periods of time, the loss of that data can impede forensic or other law enforcement activities. Specific policies related to data retention, including duration and location (e.g., user devices, cloud, or government enterprise), will need to be established.
- **Asymmetric communications:** The evolution from circuit to Internet protocol (IP)-based communications has created an asymmetric environment devoid of rules or policies to governing packet prioritization or address network congestion caused by the increased bandwidth consumption.
- **Nascent forms of communications:** The aforementioned issues are compounded with the recognition that the issue set is not limited to data exchange, but also media (e.g., pictures and video), mapping, and other emerging forms of communications.
- **Control:** Data owned by the cloud service owner and stored by the CSP is often replicated to multiple locations by the CSP as a means of data backup; however, when the data is deleted by the service owner, the original data and all replicated copies are not immediately and automatically removed. The lack of automatic removal and originator control of data can allow both well-intended and malicious actors to gain access to the data after it has been deleted by the data owner.

Infrastructure

- **Continuous monitoring:** To prevent loss of governance or control in this ad hoc and interdependent environment, it is a priority for service owners to continuously monitor into the infrastructure.
- **Surge capacity:** CSPs may have to rapidly scale resources to meet a surge in demand. The NS/EP service owner will need to ensure that all future capabilities can come online instantly and meet compliance requirements.

Resiliency

- **Ad hoc users and devices:** Managing an ad hoc user base calls for policies that extend beyond the infrastructure itself to the devices users own and operate. Assets can be lost, damaged, stolen, or otherwise unaccounted for resulting in inappropriate use, mishandling or destruction of critical data. Moreover, first responders may not be fully aware of acceptable uses of information assets, devices, or compliance requirements.
- **Incident management:** Prompt reporting of suspected or actual incidents to the proper authorities can be stymied with the vast amount of data dissemination and competing priorities during an NS/EP event. The capability to sufficiently resource the handling of a reported incident can also be compromised. Additionally, in an event when processes will likely be highly-distributed, removable media or user-installed software can

introduce malicious code into the system, device, or network without user awareness. NS/EP sponsors may want to require users and/or devices to be updated with current browsers, audio/visual equipment, and applications to reduce the chance of security issues being introduced.

Interdependency

- **Applications:** First responders increasingly rely on applications that often cannot be updated or managed effectively without access to the cloud. For example, since applications are updated on a continuous basis, not only do they require access to the cloud to receive the updates, but third parties may also need to access the application to push out patches or updates. Furthermore, the urgency of an event may not allow time to test changes and/or remediate errors before implementation, which can reduce device and application performance. Certain applications may also require increased security monitoring to prevent them from being unavailable or the target of an attack (e.g. DOS).
- **Third-party services:** CSPs that rely on third-party services or products as part of their cloud offerings may provide different levels of assurances or support many other critical functions. Additionally, impacts to the underlying telecommunications infrastructure supporting cloud services can make cloud resources unavailable.

Policy

- **Inconsistent jurisdictional requirements:** Cross-jurisdictional considerations also heighten awareness to the need for interoperability. For instance, competing jurisdictional requirements can result in challenges to comply with laws, regulations, and contracts. Currently, 47 States have different laws on data breach requirements, which can create difficulties for CSPs while developing internal policies for handling data breach incidents for both the sponsor and CSP. [40]
- **SLAs:** Contractual agreements are the current mechanism to address risks and ensure compliance with the requirements described above. Traditional SLAs and requirements definitions do not consider the criticality and uniqueness of the NS/EP environment.
- **Lack of standards:** There is an absence of robust standards and policy frameworks that account for the unique NS/EP risks. To mitigate regulatory constraints and successfully leverage the benefits of cloud computing, it is critical to develop a trust relationship in which the CSP, service owners, and even third parties clearly define and appropriately execute their respective responsibilities.
- **Responsible parties:** While CSPs and end users also have shared responsibilities for addressing risks and effectively implementing certain controls, the risk management decision is ultimately rendered by the service owners, who are accountable for authorizing and ensuring that the other responsible parties adhere to the established requirements. To compound this challenge, service agreements are often crafted by

[40] http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

individuals whose principal skills are not in acquisitions or security. In order to ensure accountability for NS/EP processes, CSPs should be subject to periodic third party audits.

2.5 Identity Assurance, NS/EP, and the Cloud

While identity in cyberspace implicates a far broader range of issues and considerations than simply those related to cloud computing, it is an issue that concerns those attempting to implement NS/EP in the cloud. Creating identity management (IdM) solutions for cloud computing will not resolve all current issues within IdM, but cloud computing will be hampered until issues of IdM in the cloud are addressed and resolved.

NS/EP cloud-based identity factors are most needed when dealing with opportunistic or event-generated criteria for mission collaboration across multiple organizations, levels of government, and private industries. These include five of the eight NS/EP mission functions the NSTAC has identified for this study, as discussed in section 3.1.

Much effort has been expended in recent years, including by the NSTAC, to develop, promote and implement IdM procedures and technologies related to the safe, secure and private application of personal identity, especially in cyberspace. The primary effort within government related to these goals is the NSTIC, which seeks to promote safe and secure assertion of identity on the Internet while preserving personal privacy and promoting interoperability between Government, civil, commercial and personal processes.[41] However, NSTIC was not created to address cloud computing, and its intended focus on business/citizen-centric online activity does not align with the special needs of NS/EP. FedRAMP's focus on streamlining Federal procurement of cloud-based services does not immediately indicate a deep background in identity assurance policy or technology. In summary, no current Federal authority directly addresses issues of identity in the cloud in a focused way.

Cloud computing's interest in IdM involves both authentication (who you are inside the cloud) and authorization (accesses and other privileges you may have relative to any given cloud, application, or data set). Both of these topics have policy and technological attributes and considerations.

Policy Issues:

As noted in section 2.2, Federal cloud computing policy authority is split between the ODNI, the CNSS, and GSA/FedRAMP. For identity authentication and authorization in the cloud, Federal organizations hosting data and applications at the FIPS 199 High Impact level and above understand the need for strong authentication by conventional trusted mechanisms. Because these organizations and their applications tend to involve the most risky identity environments in the cloud, their authorization processes are also deemed to be more secure and reliable.

[41] http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

For that reason, the focus of this discussion is on identity issues related to the NS/EP processes conducted at FIPS 199 Low or Moderate Impact levels, which coincide with the scope of FedRAMP. Cloud-identity issues are most complex at these levels because of unresolved standards for identity federation; the tendency of EP issues to straddle government/civil boundaries (and with that, limits on Government initiative to mandate solutions); the role of multi-level governmental jurisdictions in EP and incident response; and the limits on the scope and charter of existing Federal IdM initiatives. Notwithstanding that complexity, identity in the cloud for NS/EP must be addressed to find the best possible approach to this complex set of issues.

Technology Issues:

While multiple federation systems/protocols currently coexist for online IdM, none has been broadly accepted as standard.[42] This becomes a particular problem in EP situations where services and capabilities are required instantly without specific knowledge of the geography, jurisdiction, precise nature of the mission need, or knowledge of the data repositories that will need to be validated/authenticated during an event. There will be unanticipated populations of response teams, each of which will need to be able to identify themselves, communicate, and coordinate via technology as well as access various capabilities based on their roles and privileges. They will have to be accommodated in a manner that takes advantage of available technology during the event and which avoids repetition of errors and mishaps from previous events.

There is a clear link between user identity and the population of terminal devices those users employ in their work, as addressed in section 2.6. These devices may be used by responders in any situation and can be expected to have been obtained by any means, including personal/individual purchase. In many cases, upon initial acquisition, these devices are authenticated to an individual or organization (e.g., a particular fire department). Once authenticated, it may be possible to trust these devices, provided the current end-user can revalidate his/her entitlement to use the device. In such cases, the initially-established trust can be extended, resolving local issues of identifiability. However, to ensure success, both policies and technologies/devices must be configured to account for: (1) strong owner/operator authentication upon initial acquisition, even in the case of personally-owned devices intended to be used in NS/EP-response situations; and (2) streamlined end-user trust revalidation at time and place of NS/EP-response need. Note also that identity federation interoperability is not guaranteed through this process, but is an additional issue that must be addressed.

2.6 End User/Terminal Devices in NS/EP Cloud Computing

Cloud computing architecture consists of three codependent elements:

- CSPs;
- Communications conduits (carriers); and

[42] E.g.: SAML, ITML, Open ID, ID-FF. See *Glossary* for definitions.

- End user/terminal devices. (e.g., personal computers, laptops, tablets, and smartphones, not including land-mobile radios)

There are three cases for consideration of end user access to NS/EP-related data and services:

- **Traditional:** This is the approach found in legacy systems where applications and data reside in infrastructure owned, operated, maintained, and secured by government or commercial infrastructure owner/operators. These are protected by a range of systems and processes developed and refined over time to match and manage risk.[43]
- **Cloud-based:** In cloud-based architectures, CSPs are contracted to host applications, data, and services. Previous sections of this study have addressed related circumstances and needs, as well as the security responsibilities of service providers, service owners, and end users.
- **Terminal devices:** Terminal devices are becoming increasingly mobile and powerful, allowing them to host applications and large data sets within the device itself.

In spite of the rapid evolution of total performance capability by terminal devices, cloud capacity is growing faster. The trend will not be for applications and data to migrate to and become resident on devices, but for devices to be used to gain access the cloud as the venue for work performance.

Interoperability of Terminal Devices Used to Access the Cloud.

The nature of NS/EP mission functions emphasizes the trend towards an increased reliance on terminal devices, given the mobility characteristics and the ability for opportunistic use of non-dedicated hardware. It will be important for those wishing to move NS/EP missions and functions to the cloud to consider the type and nature of the terminal devices that the end user will likely access. The tendency in modern, cross-organizational work environments, including NS/EP mission functions, is towards a "bring-your-own-device" approach. This trend is increasingly driven by consumer-level purchases, which are replacing enterprise-level purchase and provision of pooled devices and resources. All end user/terminal devices must be considered, as well as the underlying operating systems that support those devices. It should be noted that some of the operating platforms to these devices are open and lend themselves to third-party vendor security applications, while other platforms are proprietary. This may pose a problem in the NS/EP context if specific device-level applications or functions are required for effective and interoperable access to the cloud services. As such, business and acquisition models that reflect these needs may require close examination.

Security of Terminal Devices Used to Access the Cloud

Cloud system security for CSPs (discussed in section 2.4) and communication conduits will in many cases be subject to regulation by the Federal Communications Commission (FCC). Security for terminal devices is exacerbated by the presumption that many end user systems will

[43] This case is not being addressed in this report.

be personally procured, owned, and maintained. While addressing the security of the terminal devices used to access the cloud is outside the NSTAC's focus, organizations wishing to move NS/EP missions and functions to the cloud should consider these issues. In addition to the interoperability issues referenced above, security considerations might incorporate the technical elements listed in Appendix I, depending on mission needs.

Interoperability and standards across defined cloud user communities remain essential considerations in achieving the potential benefits of cloud computing, especially in areas such as cross-organizational data sharing, document/work collaboration, and data analytics.

In any post-disaster recovery environment, terminal devices will be expected to interact with surviving fixed/installed information and communications infrastructure. In so doing, requirements for interoperability of such attendant network-support utilities, such as IdM, compliance monitoring and reporting, and cost capture and accounting, will exist. The ability to meet these needs is likely to vary situationally, and is not predictable.

The issue of terminal devices for NS/EP purposes within cloud-based architectures focuses needed attention on:

- **Terminal device management:** The ability for remote authorities (e.g., device vendor, operating system vendor) to remotely manipulate the device, its operating system, applications, and data, among others. For NS/EP, there would be concerns if malicious parties could access or control these functions.
- **Data/user interface evolution:** Adaptive data processing and repurposing data presentation based on user interests.
- **Intelligent infrastructure:** This near-future environment extends the relationship between user and device to cause the entire cloud infrastructure to learn from and be guided by system status, user history/activity, and session characteristics, among others. Benefits include enhanced user authentication, improved fault tolerance, and other new capabilities.

2.7 Priority Services in Cloud Computing

There are many attributes associated with the cloud that lend themselves to advancing the NS/EP mission. Under normal circumstances the cloud is ubiquitous, scalable, fully redundant, and can provide failover capabilities that are transparent to the user. Internet service provider communication networks are engineered for normal circumstances involving randomly distributed simplex link failures, while the cloud may not be available under situations involving highly-correlated or extensive damage from natural or man-made events- the very circumstances when the functionality of the NS/EP mission applications is most critical. It should also be expected that citizen demand for cloud-based services would dramatically increase under such circumstances, further compounding challenges for cloud-based NS/EP users to obtain access to vital data, services, and command and control communications.

At a minimum, ISPs must take steps to begin offering converged service capabilities and include class of service and quality of service (QoS) queues within their core and access networks. ISPs must also deploy standards-based network architectures to separate access, session management and service logic to support current and emerging technologies (e.g., long term evolution [LTE], Wi-Fi, etc.). CSPs must also implement standards-based QoS mechanisms within their cloud infrastructures to prioritize critical NS/EP applications and services over other non-NS/EP demands under adverse conditions.

If the NS/EP end user or their devices cannot access the cloud due to access network damage or congestion, there will be little to no opportunity for the end user to take advantage of the positive attributes associated with the cloud, even if they are available.

Historically, NS/EP end users accessed their systems and functions via traditional, land-line facilities; a number of protocols were established to ensure that the NS/EP user had a higher probability of accessing the network than others. As the transport/access layer has moved quickly from a circuit-switched to an IP protocol, the ability for certain types of IP traffic, specifically NS/EP, to be prioritized over normal IP traffic must be broadly implemented.

NS/EP Programs Defined:

Priority Access

The Government Emergency Telecommunications Service (GETS) is an emergency phone service provided by the National Communications System (NCS), through the Office of the Manager, NCS (OMNCS). GETS supports Federal, State, local, and tribal government, industry, and NGO personnel in performing their NS/EP missions. GETS provides emergency access and priority processing in the local and long distance segments of the Public Switched Telephone Network (PSTN). It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased.[44]

The Wireless Priority Service (WPS) is a priority calling capability that greatly increases the probability of call completion during an NS/EP event while using cellular phones. To make a WPS call, the user must first have the WPS feature added to their cellular service; no special phone is required.[45] WPS provides priority for emergency calls through a combination of special cellular network features and the same high probability of completion features used by GETS.[46]

The OMNCS has and continues to forge NS/EP standards within appropriate national and technical standards bodies. Currently, there are 14 NS/EP Telecommunications Service Functional Requirements as a requirement for the aforementioned GETS and WPS Programs of Record. The OMNCS is also developing comparable programs for the wireline and wireless,

[44] http://gets.ncs.gov/program_info.html
[45] WPS is an add-on feature subscribed on a per-cell phone basis that works with existing cell phones in WPS enabled cellular networks
[46] http://wps.ncs.gov/program_info.html

next generation IP-based networks.[47] While progress is being made in developing the protocols for the wireline backbone and next-generation LTE wireless networks, the diversity of access networks and providers is extensive. It is not clear how rapidly commercial adoption of NS/EP standards could occur and in what time-frame comparable next-generation priority IP NS/EP solutions will be deployed.

In addition, while it is recognized that NS/EP users will likely want and need to prioritize other IP services such as large-scale data and streaming media, OMNCS efforts are currently funded solely on prioritizing voice-centric packets, such as Voice over IP (VoIP).

Priority Restoration or Priority Provisioning of Access

Telecommunications Service Priority (TSP) is a program that authorizes NS/EP organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors frequently experience a surge in requests for new services and requirements to restore existing services. The TSP Program provides service vendors a FCC mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.[48]

The TSP Program has evolved over time to incorporate new types of customers that qualify for this program. The preponderance of circuits given priority restoration services are no longer government circuits, but circuits supporting service providers and other critical infrastructures that are part of the cloud. There may be a need to specifically affirm that CSPs may avail themselves of this type of priority restoration for the circuits that do support their operations and refine the current process for assigning TSP codes and their priority-levels to accommodate CSPs in general and CSPs for NS/EP functions, if a distinction should be made.

Priority Service within the Cloud

In any particular NS/EP scenario, congestion across localized telecommunications networks is anticipated. The inherent limitation of central office infrastructure, network backhaul capacity, and wireless wavelength in a particular region can be addressed through the aforementioned priority access programs. However, it is important to note that there is a difference between priority access through the telecommunications system and priority services delivered in a cloud service offering.

Government agencies, through their normal enterprise architecture planning function, have a range of options under which hosted NS/EP equities can be connected to the telecommunications network. NS/EP applications can be operated in a range of traditional or cloud-based service models, across single or multiple providers.

[47] White House "Report on the Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations", Information Infrastructure Protection Assurance Group (IIPAG) Convergence Working Group, February 2002.
[48] http://tsp.ncs.gov/

A number of cloud service providers can enable the prioritization of computing functions as a feature of their automated platforms. Under certain situations, depending upon application architecture, NS/EP application owners may find it operationally valuable to take advantage of these higher-priority computing tiers as part of certain NS/EP scenario requirements. Evaluation of how each cloud provider can enable prioritization or reduce congestion should be an essential element of any NS/EP application architecture.

Conclusion

Priority access and other existing NS/EP services are the Government's primary means to communicate during emergencies. From agencies charged with NS operations to EP responders, the need for priority access in the public networks during periods of congestion at multiple operational levels (e.g., Federal, State, and local governments and industry) to appropriately respond to incidents is paramount.

For the past 35 years, NS/EP requirements have been met using an NCS and industry partnership. The basic models for implementing and maintaining these services should continue to serve as lessons for the next generation of NS/EP and cloud challenges as the economics of convergence and IP evolution continue.

2.8 Cloud Computing Standards and Technology

To support broader Government adoption of cloud computing to support mission critical operations, incorporation of standards for interoperability, portability, and security remains paramount. U.S. laws and associated policy require Federal agencies to use international, voluntary consensus standards in their procurement and regulatory activities, except where inconsistent with law or otherwise impractical.[49] Incorporating and adhering to standards allows Government agencies to be confident of their IT solutions, ensuring competition and avoiding vendor lock-in. At the same time, development and use of robust consensus standards across the vendor and user populations enhances versatility and vibrancy of the entire public-private community engaged. Such standards, originating in the commercial sector, enhance the development and smooth application of the kinds of common SLAs advocated in this report, among other benefits.

Standards development organizations and others have created and are developing supporting cloud computing documents and related processes to include technology and standards roadmaps, conceptual models, reference architectures, taxonomies for SLAs to facilitate communication, data exchange, IdM and security for cloud computing and its application. Broader standards are emerging that focus on technologies that support cloud computing, such as virtualization. While many of these standards were developed in support of pre-cloud computing

[49] Trade Agreements Act of 1979, as amended (TAA) , the National Technology Transfer and Advancement Act (NTTAA), and The Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities

technologies, such as those designed for Web services, grid computing, and the Internet, they also support the functions and requirements of cloud computing.

New developments in technology are continuous, and influence the cloud-computing discussion. Advances in computing, especially in the areas of availability of fast central processing units, cheap memory, and advanced software for the creation, visualization and analysis of very large data sets and for trends and knowledge using data mining techniques, create new opportunities for NS/EP solutions in the future.[50]

Technological advances which focus on the importance and persistence of mobile computing and telecommunication devices coupled with a high-speed networking infrastructure are evolving the role of the mobile platform as a gateway to the cloud.

2.8.1 Big Data Analytics

There are innovation and technology trends that enhance and are enhanced by the potential for cloud computing to enable improved national priority mission services, including NS/EP. One such trend is big data analytics.

A precedent for the use of cloud computing to support NS/EP requirements was established through Japan's response to the earthquake and tsunami that struck the Greater Tohoku region in March 2011.[51.] In this example, commercially provided cloud computing services were used to help locate survivors, support situational awareness, and coordinate response.

Cloud computing can be used to facilitate the analysis of large volumes of data and therefore more complex assessments to support emergency and critical infrastructure public services on a massive scale. Collections from a broader set of sources, including terminal devices, offer the opportunity to improve the quality of NS/EP assessments. Large computing capacity, advanced software and rendering techniques combine to produce images or video, which are the result of complex modeling calculations, are easily transmitted through the communications conduit to a first responder. This culminates in enhanced and faster decisions, actions, and results.

2.8.2 Interoperability/Portability

Portability and interoperability standards are essential to the ability to establish interconnected cloud systems across CSPs, to effectively and securely support critical national priorities.

A great deal of attention has been focused on the impact of telecommunications and device incompatibilities and interoperability issues which has previously degraded first-responder efforts in communicating and coordinating responses to natural and man-made disasters. This issue is commonly cited in relation to the September 11, 2001, coordinated suicide attacks upon

[50] The importance of use, storage, access and persistence of very large datasets for the USG has been documented in *Harnessing the Power of Digital Data for Science and Society*. Report of the Interagency Working Group on Digital Data to the Committee on Science of the National Science and Technology Council, January 2009.

[51] *Responding to the Greater Tohoku Disaster, The Role of the Internet and Cloud Computing in Economic Recovery and Renewal*, Internet Economy Task Force, 2011.

the United States in New York City and the Washington, D.C. areas. The issues were reassessed because of the telecommunications response during Hurricane Katrina in 2005.

The same interoperability requirement should be considered in terms of operational software applications and data access, because of the potential use of cloud computing services to support the National Emergency Communications Plan. The objectives are to improve emergency response communications, and complementary homeland security and emergency communications strategies and initiatives.

While there is an ability to move data between CSPs and to move the workload from one provider to another, current implementations of commercial cloud services by major CSPs apply proprietary formats and constraints that prevent the seamless ability to use alternate cloud service provider software, platform and infrastructure services on demand. This can be substantiated and illustrated by the experience of significant overhead burden when moving data and software applications and/or platform services from one major cloud service provider environment to another. While portability and interoperability can be achieved, it is difficult to attain the full benefit of cloud services and the related flexibility and capacity to support NS/EP improved services.

Moreover, interoperability is needed to ensure acceptable levels of confidence in cloud availability and performance across any provider environment, on no notice, as required situationally. CSP development, adoption, and incorporation of data and service portability and interoperability standards in their products and services is a prerequisite requirement. The nature of emergency response requirements is such that the perceived risk and effort associated with movement of data and workload from one provider to another (or shared data and workload between providers) is a concern to NS/EP.

Generation of standard taxonomies for cloud computing, SLAs, and metrics need to be firmly grounded in a standard Government cloud computing architecture which will allow Government agencies to compare cloud computing services and products from different CSPs. These guidance documents and processes are key instruments for the Government to use when describing, procuring, and verifying proper receipt of contracted cloud services. These documents and processes aid in mitigating the interoperability, portability, and security risk that is associated with deployment of the emerging cloud computing model.

3.0 TASKING RESPONSES

3.1 Priorities for Cloud Migration

A primary mission of the NSTAC's study was to analyze and prioritize the migration of NS/EP-related legacy systems, services, applications and data sets to a cloud environment. This analysis was conducted using the process described below.

Figure 6[52] summarizes security risks and controls for each of the five NSTAC key factors. These risks, and controls to mitigate them, are derived from the NSTAC's security control matrices, as discussed in section 2.4 and Appendix E. The synthesis of NS/EP risks versus controls is illustrated in **Figure 7** as NS/EP issues. The figure lists the five NSTAC key factors and their corresponding NS/EP issues, adding measurable variables for each issue. For each variable, a nominal best and worst case is described.

Figure 7: Risk Management Breakout

	NS/EP Issues	(Risk Metrics) Variable	Best Case	Worst Case
Data	Data Management; User Access	Confidentiality, Integrity; Authentication	- Strong encryption, digital signature - Role/attribute-based access controls	- No encryption or integrity checks - Inconsistent/ineffective access controls
Infrastructure	Surge Capacity; Flexibility; Priority Access	Availability, Congestion, Network configure.	- Planned surge capacity - Dynamic/flexible to rapidly meet all user needs; - Comprehensive priority-access system	- No surge capability - Static/rigid system configuration - No priority access system
Resiliency	Preparedness	Recovery, Continuity, Diversity	- Well-planned and practiced procedures	- No prior planning
Interdependency	Cloud-to-cloud confidence; CI/KR confidence	Peer availability; Standards; CI/KR availability	- Complete transitivity - Full-scope availability planning	- Single-cloud isolation - No CI/KR interdependency planning
Policy/Legal	Comprehensive and consistent policies	Liability exposure; Authority stability; Jurisdictional predictability	- Clearly, precisely understood - Stable, consistent authorities - Fully understood	- No common understanding - Capricious policy changes - No visibility, predictability

Table 3 summarizes the NS/EP missions of potential relevance to cloud-based hosting. These are grouped into two categories, communications and management, with a unique number assigned to each mission category for reference.

[52] Figure 6 is located in section 2.3.

Table 3: NS/EP Mission Functions

Communications
C1 - Public broadcasts – Transmission to an unlimited audience via technical means that do not store messages (e.g. live radio or television)
C2 - Public access to information – Ability of the public to access authoritative information posted in designated data locations
C3 - Emergency coordination – Ability of emergency response personnel of all types and jurisdictions to communicate with one another for the purpose of collective NS/EP response
C4 - Emergency notifications – Transmission to a defined audience via technical means that permit data to be stored until retrieved by the user and possibly thereafter (e.g. e-mail, SMS text, recorded telephone messaging)

Management
M5 - Document collaboration – Ability for multiple persons at various locations to all see, edit, and interact on a shared document
M6 - Project coordination – Ability for multiple persons and organizations to simultaneously see and contribute to activities required for project management, including project plans and status reports
M7 - Organizational coordination – Ability for organizations to conduct meetings involving various people across any intervening space
M8 - Data archiving and storage – Ability to store and retain organizational information for backup or other purposes

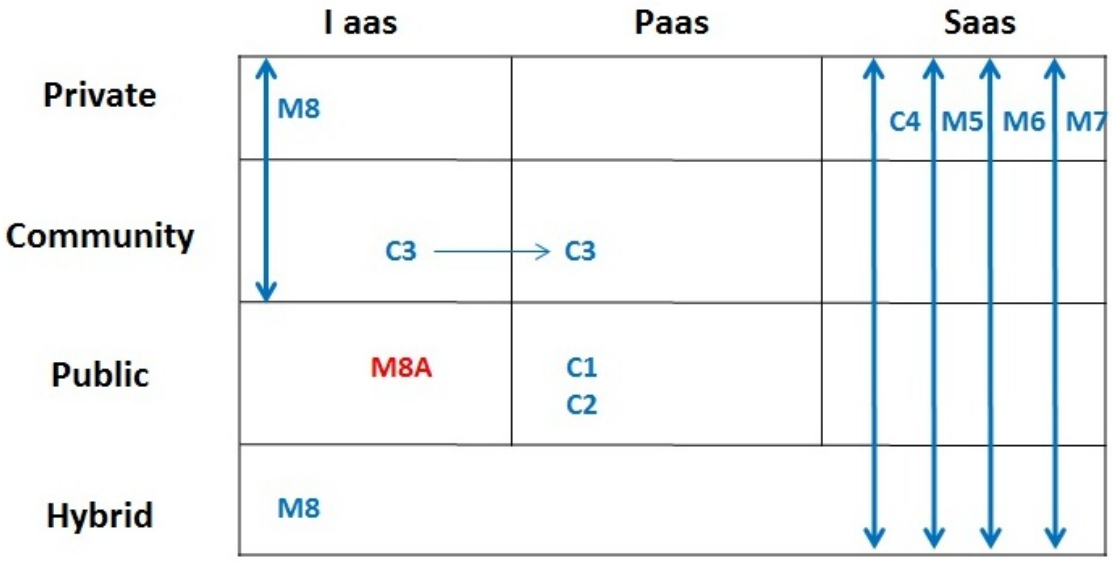
When considered in the context of the available cloud service and deployment models, certain mission functions lend themselves to specific service models due to the nature of hosted services that are available and accessed to perform the functions. These are indicated in **Table 4.**

Table 4: Mission Functions and Service Model

Mission Function	Service Model
C1 – Public Broadcasts	Platform as a Service
C2 – Public Access to Information	Platform as a Service
C3 – Emergency Coordination	Infrastructure as a Service, trending towards Platform as a Service over time
C4 – Emergency Notification	Software as a Service
M5 – Document Collaboration	Software as a Service
M6 – Project Coordination	Software as a Service
M7 – Organizational Coordination	Software as a Service
M8 – Data Archiving and Storage	Infrastructure as a Service

While it is possible to categorize optimally-indicated service models, it is not possible to prescribe or predict a specific deployment model best suited for an organization's mission in all cases. Instead, these choices are best made by potential cloud service owners, in consideration of the organization's unique factors. Since the variable involves the scope of the cloud environment, the primary question is the degree to which service owners wish to operate clouds within their own organizational boundaries, extend them to and across other organizations, or to the public. This analysis requires an examination of potential cloud applications and data sets on a case-by-case basis, which is beyond the scope of this report. These missions are depicted in **Figure 8**.

Figure 8: NS/EP Cloud Deployment/Service Model Matrix



BLUE font denotes favorably-indicated NS/EP services, applications and/or data sets for cloud migration/hosting

RED font denotes counter-indicated NS services, applications and/or data sets for cloud migration/hosting

Additional favorable indicators, not specific to mission:

- Opportunity to coordinate timing with scheduled upgrades and/or new installs;
- Opportunity to replace obsolescent and/or underperforming hardware supporting needed processes.

Additional counter-indicators, not specific to mission:

- Dedicated hardware used for system/mission backup;
- Data or processes so sensitive that their IT footprint is constrained by policy to single/stand-alone machines or defined architectures;
- Proprietary or classified data sets so sensitive their exposure would incur greater loss than benefits derived from cloud computing migration.

It is possible for service owners to design and implement some mission functions using a particular service model on any deployment models. However, some mission-deployment model pairings are counter-indicated. For example, an agency should not host sensitive data sets or applications in a public cloud. Mission function M8A has been created in order to illustrate that, in some cases, risk exposure significantly outweighs inherent advantages of cloud hosting. M8A represents hosting FIPS 199 High Impact data in a public cloud to show negative indications in the case of unwise architectural or deployment decisions. M8A has been artificially created as a control case for the model. Of note, while FedRAMP only extends from FIPS 199 Low to Moderate Impact levels, NS/EP organizations can and do conduct tailored and secure cloud-based deployments involving FIPS 199 High Impact information and processes. These management relationships, and current gaps in policy related to them, are discussed in section 2.2.

In the context of specific service models, missions are evaluated via individual NS/EP Mission-Function Score Sheets (**Figure 9**). Positive contributions to an organization's mission are scored in the values column using a 0 to +5 scale; risk exposure to the listed factor, in the case of specific missions, are scored using a 0 to -5 scale. Net scores are tabulated for each of the eight missions.

Figure 9: NS/EP Mission-Function Score Sheets
Blank Mission-Function Score Sheet

Mission Function

	NS/EP Issues	Variable	Value (0/5)	Risk (0/-5)	Net
Data	Data Management;	Confidentiality, Integrity;	_____	_____	_____
	User Access	Authentication	_____	_____	_____
Infrastructure	Surge Capacity;	Availability, Congestion, Network configure.	_____	_____	_____
	Flexibility;				
	Priority Access				
Resiliency	Preparedness	Recovery, Continuity, Diversity	_____	_____	_____
Interdependency	Cloud-to-cloud confidence;	Peer availability; Standards;	_____	_____	_____
	CI/KR confidence	CI/KR availability	_____	_____	_____
Policy/Legal	Comprehensive and consistent policies	Liability exposure;	_____	_____	_____
		Authority stability;	_____	_____	_____
		Jurisdictional predictability	_____	_____	_____
		Totals	____	____	____

Blank Mission Function Score Sheet With Key

Mission Function

	NS/EP Issues	Variable	Value (0/5)	Risk (0/-5)	Net
Data	Data Management;	Confidentiality, Integrity;	___1V____	___1R____	_____
	User Access	Authentication	___2V____	___2R____	_____
Infrastructure	Surge Capacity;	Availability, Congestion, Network configure.			
	Flexibility;		___3V____	___3R____	_____
	Priority Access				
Resiliency	Preparedness	Recovery, Continuity, Diversity	___4V____	___4R____	_____
Interdependency	Cloud-to-cloud confidence;	Peer availability; Standards;	___5V____	___5R____	_____
	CI/KR confidence	CI/KR availability	___6V____	___6R____	_____
Policy/Legal	Comprehensive and consistent policies	Liability exposure;	___7V____	___7R____	_____
		Authority stability;	___8V____	___8R____	_____
		Jurisdictional predictability	___9V____	___9R____	_____
		Totals	____	____	____

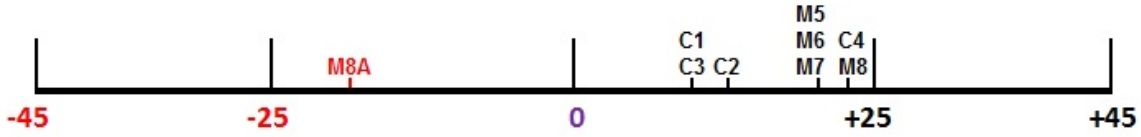
Mission-Function Score Sheet Attribute Descriptions

	Value (V)	Risk (R)
1	To what extent can data confidentiality and integrity be assured?	To what extent would lack of data confidentiality and integrity damage the mission?
2	To what extent can user access be confidently authenticated and access to hosted data and/or processes controlled accordingly?	To what extent does or would loss of user/access authentication damage mission performance?
3	To what extent would networks relied upon for mission functions confidently be available, even under adverse conditions and based on unanticipated demands?	To what extent would mission performance be damaged in the event of network congestion or temporary unavailability?
4	To what extent does this mission anticipate and account for diverse and/or alternative means, paths and processes in the interest of ensuring continuity of service?	To what extent is mission performance dependent upon rapid and efficient network reconstitution after a degrading event?
5	To what extent does mission performance anticipate and account for standards and interoperability across disparate IT regimes?	To what extent is mission performance dependent upon external IT networks/architectures, including interoperable standards?
6	To what extent are CI/KR co-dependencies essential to mission performance anticipated in planning and accounted for as contributing capabilities?	To what extent does the mission depend upon sustained and reliable performance of co-dependent CI/KR over large areas?
7	To what extent do mission planning and authorities inoculate service owners from liability exposure?	To what extent does potential legal liability increase when migrating from legacy to selected cloud-based environments?
8	To what extent is the mission underpinned by sufficiently-comprehensive and stable authorities?	To what extent does the mission risk disruption by adverse acts of authority at any level?
9	To what extent can jurisdictionally-specific compliance and/or reporting requirements be confidently anticipated?	To what extent is mission performance subject to unpredictable, dynamic or diverse legal and regulatory requirements?

Using a scoring system, any positive contribution to mission performance must be evaluated alongside negative risk factors. If both scores are high or low, the values and risks are balanced and a deployment decision is not strongly indicated. In cases where evaluations are mostly positive, these missions are most favorably indicated for cloud migration. Missions whose attribute scores are less positive, while still favorably indicated for cloud migration, should be pursued as a lower priority.

The Cloud-Migration Scoring Summary lists scores for all NS/EP cloud computing mission-function candidates, as shown in **Figure 10**.

Figure 10: NS/EP Cloud Migration-Scoring Summary



Label	Mission Function	Service Mdl	Deployment Mdl
C1	Public Broadcast	(P)	(Public)
C2	Public Access to Information	(P)	(Public)
C3	Emergency Coordination	(I→P)	(Community)
C4	Emergency Notification	(S)	(All)
M5	Document Collaboration	(S)	(All)
M6	Project Coordination	(S)	(All)
M7	Organizational Coordination	(S)	(All)
M8	Data Archiving & Storage	(I)	(Private, Community, Hybrid Priv/Comm)
M8A	Data Archiving & Storage	(I)	(Public, Hybrid w/Pub) **(CONTROL CASE)**

The scoring summary reflects the NSTAC findings that:

- Presuming wise architectural decisions regarding deployment and service model choices, including appropriate attention to security, NS/EP functions are generally amenable to migrating to cloud-based processes.
- In considering cloud migration, it is possible to make poor architectural choices resulting in acceptance of risks that outweigh benefits.
- The key consideration is how a given equity should be migrated to the cloud.
- In NS/EP applications, potential cost savings are secondary. These can only be predicted and realized after calculating full-scope performance improvements against changes in direct security costs and imputed risk exposure, all on a case-by-case basis. Recognized NS/EP benefits will come in the form of improved mission performance.
- Those NS/EP missions that are limited in scope to and throughout Government and other defined critical infrastructure and key resources (CI/KR) communities appear more attractive for cloud migration than those which extend to the public or invite public access.
- Those mission functions which appear most attractive for cloud migration, as depicted on **Figure 10,** should be considered for earliest programmatic action, instead of those where the mission benefit based on risk-benefit analysis is less attractive.

3.2 Special Requirements for Providers Hosting NS/EP-related Equities

As processes migrate to a cloud-based environment, roles of traditional security service providers also evolve, with a conceptual split between NS and EP.

NS systems are categorized as under ODNI or CNSS management. Neither of these categories of systems is managed within the scope of FedRAMP's policy authority.

Management of cloud computing within and across the IC is migrating to the ODNI. At present, five IC organizations comprise the "IC Quint" of participants in IC-cloud architecture.[53] Community planning has identified 11 "service areas" which are in the process of being awarded to various IC organizations for leadership – four such awards have already occurred.

Basic characteristics of IC cloud use include:

- No public clouds (other than limited pilot projects and concepts);
- Retention of network security functions in-house, regardless of service or deployment model;
- No significant role in emergency preparedness, as defined here; and
- No current FIPS 199 clouds. There are future intentions to collaborate with the Defense Information Systems Agency.

Of the specific NS/EP Mission Functions listed on **Table 3**, all eight of these functions are performed within the sphere of emergency preparedness, but only the four "M"-series missions (M5-M8) within the NS community/domain.

Within these parameters, the IC is carefully calculating which equities and processes to migrate to a cloud-based environment. By focusing on selecting specific cloud service and deployment models, in-house security-service oversight, and close control over cloud access (via existing IC identity authentication and authorization processes), it is working to mitigate many of cloud computing's risk factors. In that regard, the IC's use of cloud technology may be considered a special case, relative to the basic model of commercial outsourcing of governmental processes to vendor-provided hosting services.

As previously noted, the Secretary of Defense, as chair of the CNSS, has cognizance over cloud computing for national security systems generally. FedRAMP currently embraces FIPS 199 Low and Moderate Impact systems, which comprise 41 percent and 47 percent of FISMA-reported systems, respectively.[54] The majority of EP systems and processes eligible for potential cloud migration would fall under this management structure. The cloud security controls developed by the NSTAC, described in section 2.4 and listed in Appendix E, are intended for the Secretary of Defense and OMB to consider applying to organizations and systems under their

[53] NSA, CIA, DIA, NRO and NGA

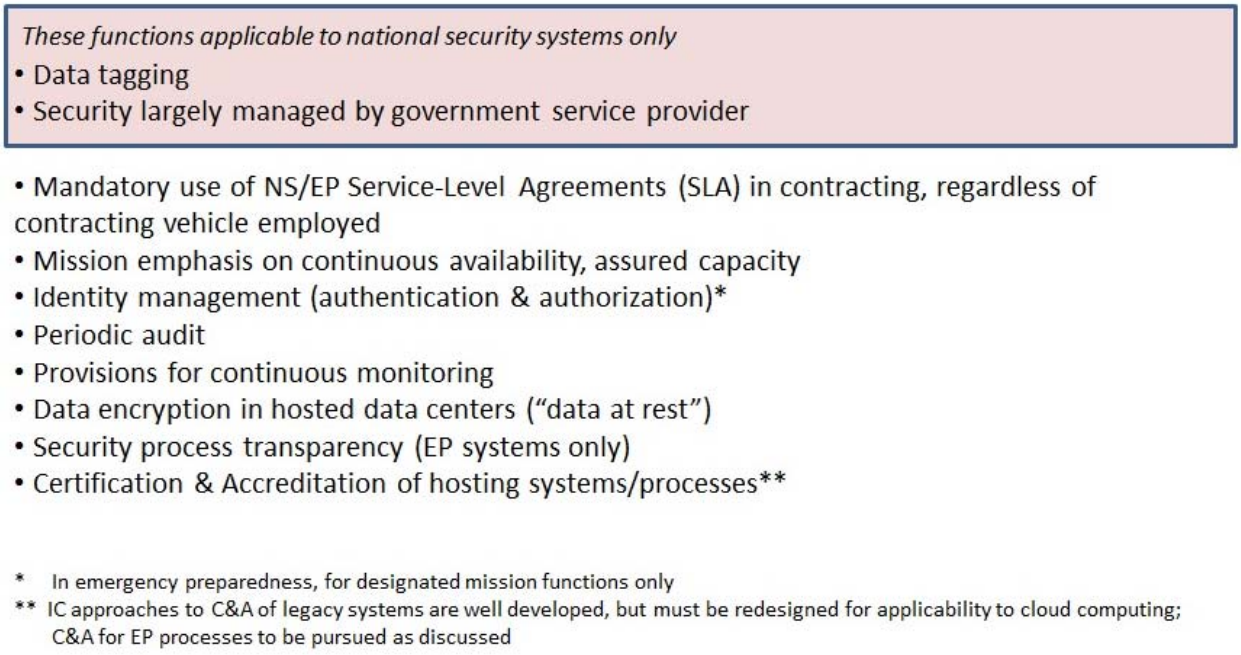
[54] Office of Management and Budget, *Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*, pg 28.

management authority. These controls represent best-of-breed insights from the governmental, industry, audit and international cloud communities, all portrayed in common format and specifically tailored to key priorities, issues and concerns of NS/EP. As such, they represent an opportunity to approach and measure cloud security for NS/EP in a consistent and extensible way, manageable across all policy frameworks. In the case of OMB, this is consistent with existing FedRAMP policies, which provide for the establishment of additional security controls and structures for (defined needs or purposes) known as supplementing the tailored baseline.[55]

Considering the criticality of NS/EP missions and functions, the NSTAC identified the need for a program of security processes specific to NS/EP equities. The elements of a properly-structured security framework are summarized in **Figure 11**. The two items inside the box are applicable to NS systems managed within the IC only; the remaining listed items are deemed applicable to both NS and EP systems.

The specific measures outlined in **Figure 11** and reflected in sections 4, 5 and 6 should be implemented collectively in the context of a NS/EP cloud computing strategy, in the form of a package of SLA's for all NS/EP cloud hosting, to be created and managed in partnership with appropriate industry service providers and NS/EP service owners.

Figure 11: NS/EP Cloud-Security Service Requirements



[55] NIST SP 800-53 R3, Page 23, Supplementing the Tailored Baseline.

4.0 FINDINGS

Cloud computing offers significant benefits that are readily visible and often measureable. It also contains risks, both natural and manmade, which are more difficult to measure. In addition to classic cybersecurity risks and threats, cloud computing adds new risks resulting from unpredictability in terms of venue, proximity to threats, and the performance of remote managers entrusted with cloud-based resources. Understanding risks and threats in cloud computing will not only help advance cloud technologies but also allow organizations to implement specific policies and managerial practices to mitigate the risks. With these assurances in place, cloud computing migration may proceed by conscious risk-benefit calculation.

Parenthetical paragraph notations preceding individual points in the next three sections (Findings, Conclusions and Recommendations) refer to the section of the basic text from which the points are adduced. Specific findings (plus conclusions and recommendations to follow) are grouped topically into three categories: Strategy, Policy and Structure; Security; and Technology.

Strategy, Policy and Structure:

- (2.0) Plans and programs must be attuned to the emergence of new technologies with potential to impact cloud computing efficiency, security and/or value. As new technologies emerge, plans and programs must be prepared to adapt appropriately.
- (2.0) Cloud computing implicates preexisting policies, plans and strategies related to security, privacy and identity management. These processes impact NS/EP. If these related processes are not closely examined for the potential effects of cloud computing on them, the result may be degraded functionality versus planned standards and new risk exposures.
- (2.0) The current attention to privacy in public policy is focused on commercial activities, since that is where the majority of PII is exposed and at risk. These issues are not within the scope of NS/EP. However, it is possible that in future, issues of NS/EP concern related to privacy will emerge.
- (2.1) The existing NS/EP definition, as reflected in 47 CFR 201.2(g) is inadequate as regards cloud computing, in that it omits any reference to several aspects of cloud-based processes critical to NS/EP, to include data at rest. In the case of cloud computing, NS/EP-critical data sets may be resident in clouds of any kind, and potentially exposed to the whole range of security hazards.
- (2.1) Differing treatment of legal issues critical to cloud computing across jurisdictional boundaries leads to instability and reduced confidence in measured risk exposure in a cloud environment. Data-breach standards and sanctions are one such example.

- (2.1) Multiple contracting vehicles are available for federal cloud-service procurement, but currently only the GSA Networx contract includes SLAs which define and provide for NS/EP-related assurances specifically.
- (2.2) FedRAMP is designed to provide a centralized process for security accreditation of cloud computing services at the low and moderate impact levels under FIPS 199. The ODNI has created cloud-management processes across the intelligence community, and the Secretary of Defense is responsible for all national security systems. However, since FIPS 199 expressly excludes national security systems, a gap in oversight and management exists in the case of FIPS 199 High Impact level systems, of which there were 2315 identified in the 2009 FISMA report to Congress.
- (2.3) It is possible to map NS/EP-focused issues, interests and concerns within the larger subject of cloud computing. In so doing, certain NS/EP-specific cloud insights and priorities emerge that may not be identical to those of cloud computing generally.
- (3.1) Organizations with key NS/EP roles should first consider private-cloud implementations as a means of gaining experience and refining policies and procedures. When ready, they should then consider expanding their cloud architecture into more complex cloud structures, if deemed appropriate.
- (3.1) As regards migration of legacy NS/EP equities to cloud-based environments, the NSTAC finds that:
  - Presuming wise architectural decisions regarding deployment/service models, including appropriate attention to security as discussed above, NS/EP functions are generally amenable to migration to cloud-based processes, some more so than others.
  - In considering cloud migration, it is possible to make poor architectural choices resulting in acceptance of risks that outweigh benefits.
  - Thus, the key consideration is how a given equity should be migrated to the cloud.
  - In NS/EP applications, potential cost savings are secondary. In any case, these can only be predicted and realized after calculation of full-scope performance improvements against changes in direct security costs and imputed risk exposure, all on a case-by-case basis. Recognized NS/EP benefits will come in the form of improved mission performance.
  - Those NS/EP missions that are limited in scope to and throughout Government and other defined CI/KR communities appear more attractive for cloud migration than those which extend to the public or invite public access.
  - Migration of NS/EP equities to the cloud should only occur under appropriate oversight and policy supervision. .
  - Those mission functions which appear most attractive for cloud migration, as depicted on **Figure 10**, should be considered for earliest programmatic action, in favor of those where the mission benefit based on risk-benefit analysis is less attractive.

- (3.2) NS/EP-related cloud migrations must be conducted within the framework of a comprehensive security strategy, including relevant provisions for technology, process and human factors. This strategy may be implemented through a system of service-level agreements, made mandatory for all NS/EP cloud-service contracting.
- (3.2) Cloud computing services and service providers vary widely. The best way for NS/EP-sensitive activities to be confident of predictably-secure performance at required levels is through a comprehensive security program including security controls, audits, continuous monitoring and C&A of NS/EP cloud-use systems. In NS environments, additional measures may be deemed appropriate. Taken together, these measures may have the desired effect of stabilizing security architectures and services. Transparency and visibility of security processes by all involved in a cloud environment are essential to build confidence in the integrity of the security regime.

Security:

- (2.4) NS/EP represents a special case within cloud computing, with risk-tolerance factors and weighted values for availability, authenticity, etc. that are not the norm for utility computing applications. These considerations require NS/EP authorities to carefully consider the implications and effects of reliance upon cloud-based processes in the performance of vital NS/EP missions.
- (2.4) Cloud computing remains closely associated with classic forms and practices of cybersecurity, and the magnitude of the cybersecurity threat to cloud-based processes may not be greater or lesser than that faced by conventional networks and data. That said, the nature and range of threats to cloud computing are unprecedented in several important areas. As such, classic plans, programs, procedures and policies designed to protect information systems are often ill-prepared to operate in a cloud environment, unless consciously and thoughtfully adapted to new requirements, metrics and threats. Careful examination is required to ensure that thoughtfully planned approaches to implementation properly balance benefits and risks.
- (2.4) Cloud computing migration risk decisions cannot be made solely on the basis of the particular cloud service or deployment model to be used. While these contribute to the total risk calculus, that analysis must also consider security controls in use, and the ways in which these are rigorously validated and audited.
- (2.4) An ideally-constructed set of cloud computing security controls for NS/EP must embrace the experiences, insights, needs and views of government, industry, professional auditors and prospective partners both at home and abroad.
- (2.4) As a result of policies or decisions made by vendors or subcontractors, NS/EP-relevant data and processes may be exposed to the cloud without the customer having consciously subscribed to it, or even being aware of the change in his risk profile.
- (2.4) Cloud-deployment decision analysis by NS/EP service owners should focus on mission considerations, both in terms of potential new functionality and possible enhancement to the performance of existing missions. Cost measures in cloud migration

are unpredictable before the fact, and should be secondary considerations in NS/EP cloud migration in any case.

- (2.4) Cloud instantiations are relatively insensitive to content and specific data sets, in that benefits are largely measured in terms of savings in hardware, infrastructure and headcount. As such, a potential cloud deployment involving highly sensitive information or processes might be seen as practically identical, in terms of benefit, to a similarly-scoped cloud deployment intended to embrace information of no sensitivity at all. However, the consequences of potential compromise of those respective data sets make the risks associated with these two examples enormously different. Therefore, the net value assessment may support cloud migration in one case and not the other.
- (2.4) Some of the potential benefits of cloud computing relevant to NS/EP are not easily measured before the fact. These include extensibility of architectures; access to unexpected correspondents, at unpredictable times, on short notice; increased efficiency in design and operations of data centers; etc. Still other benefits may become understood and exploitable over time, in the form of new functionalities and/or new approaches to established missions. Security risk is classically difficult to measure and quantify. Thus, arriving at consistent and reproducible findings of net value in cloud computing implementation will be based on at least some assumptions that will resist accurate measurement.
- (2.4) Loss of cloud-hosted data and other content is risked if and when cloud-service providers go out of business. Poorly-designed and implemented data-backup strategies by CSP's can have the same effect. However, there is a lack of standards to ensure portability of cloud-hosted content between and among clouds hosted by different providers.
- (2.4) Multiple organizations in Government and industry have created security-controls frameworks for cloud computing. While several of these are relevant to NS/EP, until now none has been created or adopted for NS/EP purposes specifically.
- (2.5) Identity requirements in support of NS/EP cloud activities must be assessed on an individual-mission basis. Some NS/EP mission functions are very identity-sensitive, others hardly at all.
- (2.5) Current boundaries of topical scope, professional focus and domain knowledge are such that the subject of identity-in-the-cloud (NS/EP or otherwise) is not yet fully addressed by the federal government. This situation is a concern for emergency preparedness missions and functions in particular.

Technology:

- (2.6) Cloud computing, as accessed and used in support of NS/EP missions, is comprised of three elements: The data centers; communications conduits; and end-user terminal devices.
- (2.6) Cloud computing shares a characteristic with legacy systems, especially as regards emergency-preparedness response: Dependence on last-mile end-user technologies, existing largely outside of any central policy or programmatic control. Total cloud

system performance, responsiveness and value for NS/EP purposes is dependent on these endpoint technologies, collectively.

- (2.7) Current Federal programs for priority restoration or provisioning and do not necessarily extend to or incorporate all cloud computing scenarios.
- (2.7) A distinction exists between priority access programs and priority service features within the cloud. Whereas access to telecommunications networks may be limited by localized congestion, prioritized services within the cloud can be architected across a wide range of providers and options.
- (2.8) Standards work in cloud computing is progressing, but current/remaining gaps of potential interest and concern to NS/EP are not currently evaluated or understood in a focused way.

5.0 CONCLUSIONS

As the Government executes its Cloud First policy, NS/EP mission migration should proceed in accordance with the priorities and processes outlined in section 3.1 of this report. Such migration should be conditioned upon adoption of the security-related SLA's for NS/EP-in-the-cloud outlined in section 3.2.

Strategy, Policy and Structure:

- (2.0) If Federal plans and programs related to security, privacy and IdM are not reexamined in the context of changes precipitated by cloud computing, they risk missing important new relationships and understandings important to the processes they seek to manage.
- (2.1) In order to properly encompass the full scope of the intersection of cloud computing and NS/EP, the official definition of NS/EP now reflected in the CFR should be expanded to embrace information services, as defined in U.S. code and the CFR.
- (2.1) Jurisdictional considerations, both foreign and domestic, are a matter of concern to NS/EP in cloud computing. These uncertainties may inhibit initiative of some NS/EP service owners to support cloud migration.
- (2.1) NS/EP mission contracting should require NS/EP-related SLAs of the type found in the GSA Networx contract vehicle. These SLAs should be maintained and updated in consideration of continuously evolving threats and emerging technologies.
- (2.2) The current policy gap in Federal cloud computing, defined by systems at the FIPS 199 High Impact level, could result in inefficient and slower adoption of cloud services for certain EP functions. Specifically, if the same cloud based EP systems are being certified in the cloud by multiple agencies, then a centralized certification process may save the government time and money as well as increase the adoption of cloud services. The gap does not mean high impact EP systems could not operate in the cloud since agencies could conduct their own security assessment and authorization outside of

FedRAMP as they do today. However this approach perpetuates the problem FedRAMP was conceived to solve, where multiple assessment and authorization processes are applied to the same cloud systems by multiple agencies.

- (3.1) Full analysis of NS/EP mission functions demonstrates that some missions are more amenable to cloud migration than others. If security, contracting and other controls, as described throughout this study, are put in place, migration of certain NS/EP missions/functions to cloud-based environments may proceed with reasonable confidence of positive net-value.
- (3.2) There are specific security and other requirements which should be in place as conditions for support to migration of NS/EP-related equities to the cloud. These can be identified, and should be managed as part of a comprehensive NS/EP cloud security strategy, created and managed by the NCS.

Security:

- (2.4) It is possible to analyze cloud computing in terms of security threats that are both traditional and new. A vital aspect of cloud migration or adoption of new cloud services will be the establishment of a comprehensive security regime tailored to the nature of cloud computing and the specific missions contemplated. This analysis must consider deployment and service model choices, nature of data/services, intended user population, and many other factors. In this process, mission needs and performance considerations must be foremost.
- (2.4) NS/EP service owners have to acquire new processes for risk management in the cloud computing environment. Effective adoption will require new skill sets to overcome longstanding Federal information security weaknesses identified in agencies' annual FISMA reports to Congress and overcoming challenges with effective change management. Service owners have to address traditional information security problems in an evolving technological domain, which requires developing and implementing new controls or modifying existing ones to adapt to this dynamic environment.
- (2.4) The NSTAC cloud security controls matrix developed in this report has been informed by controls used by the CSA, ISACA, ENISA and FedRAMP, which in turn embraces controls in NIST SP 800-53.
- (2.5) NS/EP mission confidence and performance would benefit from rationalization of identity management federation standards across the community of interest. This would involve, above all, selection of a single-format identity federation broker for NS/EP purposes. It may be possible to do this for defined NS/EP missions and functions, even while not seeking to extend this model to aspects of the national Identiverse not involved in NS/EP.
- (2.5) Attention to strong user authentication of IT devices expected to be used in NS/EP situations would permit trust in these devices upon revalidation of their users in response situations.

Technology:

- (2.6) Federal NS/EP cloud strategies must embrace the role of terminal devices/users as part of the total NS/EP cloud architecture.
- (2.7) A service-restoration and provisioning process analogous to TSP should be extended to cloud providers as a means to ensure cloud computing as a reliable mechanism for support to NS/EP mission functions.
- (2.7) The availability (or lack thereof) of priority access for the NS/EP end user devices, particularly IP-based devices should be understood in making the determination to move NS/EP missions to the cloud.
- (2.8) Development of standards to meet specific needs in cloud computing are required as a matter of urgency.
- (2.8) There is both need for and value in security research specifically focused on the cloud computing environment.

6.0 RECOMMENDATIONS

6.1 Highest-Priority Presidential Recommendations:

The President's National Security Telecommunications Advisory Committee (NSTAC) recommends that the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, undertake the following package of actions as a matter of the greatest priority related to national security and emergency preparedness (NS/EP) in cloud computing:

- Direct the appropriate Government organization to develop processes and maintain priorities as described in the body of the report for migration of NS/EP missions to cloud based environments.
- Direct the adoption of NS/EP service level agreements (SLA) in all contracts pertaining to NS/EP cloud computing, which address the following functionalities:
  - Mission emphasis on continuous availability, assured capacity;
  - Identity management (authentication & authorization) for specified mission functions;
  - Periodic third-party audit;
  - Provisions for continuous monitoring;
  - Data encryption in hosted data center (data at rest);
  - Security process transparency for users (EP systems only); and
  - Certification and Accreditation (C&A) of hosting systems/processes.

  - For certain national security systems, additional requirements include:
    - Data tagging; and
    - Security management conducted by government service provider.

- Direct the National Communications System (NCS) to adopt cloud security controls developed by this study and found at Appendix E as a comprehensive NS/EP cloud security program, making their use mandatory by NS/EP service owners and auditable by third parties.
- Broaden the definitional scope of NS/EP, as reflected in current law and federal regulation, to embrace information services, as defined, in order to permit the technical nature of cloud computing to fit within the NS/EP definition.
- Direct the expansion of scope of the Federal Risk and Authorization Management Program (FedRAMP) to embrace those governmental information systems reportable under the Federal Information Security Management Act (FISMA) as being of Federal Information Processing Standards (FIPS) 199 High Risk Impact level, thereby closing a current gap in oversight of a large number of systems relevant to NS/EP.
- Direct the initiation of a Federal program, in collaboration with relevant industry partners, to develop a system for priority access to cloud-based equities in times of need, based on infrastructure degradation due to natural or man-made causes.

6.2 Additional NSTAC Recommendations to the President:

In addition, the following recommendations are provided:

Strategy, Policy and Structure:

- (2.0) Examine existing Federal plans and programs for security, privacy and identity management relevant to NS/EP, all in terms of the effects of cloud computing on them. Adjust those plans as appropriate based on review.
- (2.1) Prior to permitting any NS/EP data to be moved to cloud services where the cloud service provider (CSP) may store the data in servers located on foreign soil, conduct an examination of the data laws for foreign countries and only proceed if the results indicate acceptably-robust protections for such data.

Security:

- (2.5) Direct the Department of Homeland Security (DHS), in coordination with the General Services Administration (GSA) and other Federal agencies with significant cross-jurisdictional identity-sensitive NS/EP missions, to conduct a selection analysis and pick the most appropriate currently-available identity management protocols for mandatory use in all NS/EP missions and functions.

Technology:

- (2.6) Implement a program, through DHS, of authentication of mobile information technology (IT) devices used in NS/EP-response situations, such that user identity can be quickly revalidated, permitting their trust in use. Secure Remote Access to the cloud for NS/EP users must meet a stringent set of security conditions laid out in section 2.6.
- (2.7) Accelerate the current Office of the Manager, National Communications System (OMNCS) initiatives, in collaboration with appropriate industry partners, to develop next generation Internet protocol (IP)-based priority services. Incorporate mechanisms to assure priority access of transport to cloud-based services and activities related to NS/EP.
- (2.7) Determine the feasibility of leveraging the existing Telecommunications Service Priority (TSP) program to create a nationwide process for prioritization of provisioning and restoration of cloud services in the event of congestion, saturation and/or outages from whatever cause, which effect NS/EP services or equities. If such a project is deemed feasible, develop a proposed plan for implementation in appropriate detail.
- (2.7) Encourage NS/EP application architects to evaluate cloud service platforms that include congestion-avoidance features such as geographic load balancing or priority service tiers.
- (2.8) Direct the National Institute of Standards and Technology (NIST) to collaborate with other government and industry stakeholders to develop security standards for cloud computing applicable to NS/EP cloud-based functions.
- (2.8) Permit NS/EP data and other content to be hosted only by service providers who support broad portability based on open standards between cloud types and service providers.
- (2.8) Direct NIST to develop cloud data format and portability standards as a matter of priority.
- (2.8) Create and manage innovation-laboratory cloud(s), isolated from core processes to prevent risk of disruption, to support security research related to cloud computing and facilitate development of new cloud applications and user functions. This should be done in public, private, and community deployment models.

APPENDIX A

SUBCOMMITTEE MEMBERS, SUBJECT MATTER EXPERTS, AND SUBCOMMITTEE MANAGEMENT

APPENDIX A: SUBCOMMITTEE MEMBERS, SUBJECT MATTER EXPERTS, AND SUBCOMMITTEE MANAGEMENT

SUBCOMMITTEE MEMBERS

Palo Alto Networks, Incorporated	Mr. Mark McLaughlin, Chair Mr. William Gravell, Working Group Leader
AT&T, Incorporated	Ms. Elizabeth Gunn
Avaya, Incorporated	Mr. Siafa Sherman
Blue Ridge Networks	Ms. Joan Grewe
CenturyLink, Incorporated	Ms. Kathryn Condello Mr. Martin Capurro Mr. Michael Glenn Mr. Waqar Khan
Cisco Systems, Incorporated	Mr. Vinay Bansal
Communication Technologies, Incorporated	Mr. Milan Vlajnic
CSC	Mr. Guy Copeland Mr. Robert Kondilas Mr. Dean Weber
Department of Commerce	Mr. Robert Bohn Ms. Dawn Leaf
Department of Defense	Mr. Wayne Farmer
Department of Justice	Mr. Steve Chabinsky
General Services Administration	Mr. William Lewis
Harris Corporation	Mr. Jim Leach
Juniper Networks, Incorporated	Mr. Robert Dix
Level 3 Communications, Incorporated	Mr. William Ramthun Mr. Nick Taylor

McAfee, Incorporated	Mr. Edward White
Microsoft Corporation	Mr. Paul Nicholas Ms. Min Hyun
Neustar, Incorporated	Ms. Terri Claffey
Raytheon Company	Mr. William Russ
Sprint Nextel Corporation	Mr. Perry Siplon
Telcordia Technologies	Mr. Joseph Bednar Ms. Louise Tucker
Terremark Federal Group	Mr. Norman Laudermilch Mr. Donald Tighe
tw telecom, Incorporated	Mr. Michael Gearin Mr. Colin Gosnell
Verizon Communications, Incorporated	Mr. Marcus Sachs

SUBJECT MATTER EXPERTS

AT&T, Incorporated	Ms. Rosemary Leffler
Booz Allen Hamilton	Mr. Perry Bryden
CenturyLink, Incorporated	Mr. David Shacochis
Juniper Networks, Incorporated	Mr. Scott Sneden Mr. Purvin Vakharwala
VeriSign, Incorporated	Mr. Danny McPherson Mr. Rick Howard

SUBCOMMITTEE MANAGEMENT

Designated Federal Officer	Mr. James Madon
Alternate Designated Federal Officer	Mr. Michael Echols Mr. Allen Woodhouse
Department of Homeland Security	Ms. Sandra Benevides
Booz Allen Hamilton	Ms. Laura O'Reilley Ms. Melissa Zientek

APPENDIX B:

ACRONYMS

APPENDIX B: ACRONYMS

CCSS	Cloud Computing Scoping Subcommittee
CFR	Code of Federal Regulations
CI/KR	Critical Infrastructure and Key Resources
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DFO	Designated Federal Official
DHS	Department of Homeland Security
DNS	Domain Name System
DOD	Department of Defense
DOS	Denial-of-Service
ENISA	European Network and Information Security Agency
EOP	Executive Office of the President
FCC	Federal Communications Commission
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Systems Management Act
GETS	Government Emergency Telecommunications Service
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive

IaaS	Infrastructure as a Service
IC	Intelligence Community
ID-FF	Identity Federation Framework
IdM	Identity Management
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISP	Internet Service Provider
IT	Information Technology
ITAR	International Traffic in Arms Regulations
ITML	Information Technology Markup Language
LTE	Long Term Evolution
NCS	National Communications System
NGO	Non-Governmental Organization
NIST	National Institute of Standards and Technology
NS/EP	National Security and Emergency Preparedness
NSD	National Security Directive
NSPD	National Security Presidential Directive
NSTAC	National Security Telecommunications Advisory Committee
NSTIC	National Strategy for Trusted Identities in Cyberspace
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OMNCS	Office of the Manager, National Communications System
QoS	Quality of Service

PaaS	Platform as a Service
PII	Personally Identifiable Information
PMEF	Primary Mission Essential Function
PSTN	Public Switched Telephone Network
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SP	Special Publication
TSP	Telecommunications Service Priority
VoIP	Voice over Internet Protocol
WPS	Wireless Priority Service

APPENDIX C:

GLOSSARY

APPENDIX C: GLOSSARY

Broad Network Access: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs). (NIST SP 800-145)

Bring-Your-Own-Device: A type of rate plan offered by some mobile phone and VoIP service providers, for customers who want to use their own existing mobile phone or VoIP device, respectively, when they sign up with a new service provider. BYOD plans typically have no term commitment, no early termination fee, and possibly even a lower monthly recurring charge than the service provider's other plans, all of these concessions made possible by the service provider's not having to incorporate a subsidy for a "free" instrument into the rate plan. (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 SP 800-145)

Cloud Security Alliance (CSA): A not-for-profit organization with a mission to promote the use of best practices for providing security assurance within Cloud Computing, and to provide education on the uses of Cloud Computing to help secure all other forms of computing. The Cloud Security Alliance is led by a broad coalition of industry practitioners, corporations, associations and other key stakeholders. (Cloudsecurityalliance.org)

Cloud Service Consumer: The end user that actually uses the service, whether it is Software, Platform or Infrastructure as a Service.

Cloud Service Owner: The entity that acquires cloud services such as Platform or Infrastructure as a Service from a Cloud Service provider then adds components/configuration to deliver the required mission functionality to the cloud consumer.

Cloud Service Provider: A government or commercial entity that has offers cloud services to external organizations.

Communications Conduit: The way a user achieves access to the cloud periphery.

Community Cloud: The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise. (NIST SP 800-145)

Critical Infrastructure and Key Resources (CI/KR): An interdependent network of vital physical and information facilities, networks, and assets, including the telecommunications,

energy, financial services, water, and transportation sectors, that private business and the Government rely upon (including for the defense and national security of the United States). Critical infrastructures are those systems and assets so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security (including national economic security) and/or national public health or safety. (Federal Continuity Directive 1)

Data: This is AT&T Bell Labs' definition: "A representation of facts, concepts, or instructions in a formalized manner, suitable for communication, interpretation or processing." Typically anything other than voice. (Newton's Telecom Dictionary)

Denial of Service: You're no longer allowed to use a service. That service might be anything from normal phone service (you didn't pay your bills) to not being allowed into the company's email because you were just fired. (Newton's Telecom Dictionary)

Deployment Model: The manner in which a given entity is implemented.

European Network and Information Security Agency (ENISA): Working for the EU Institutions and Member States. ENISA is the EU's response to these cyber security issues of the European Union. As such, it is the 'pace-setter' for Information Security in Europe, and a centre of expertise. (enisa.europa.eu)

Federal Risk and Authorization Management Program (FedRAMP): A Government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a "do once, use many times" framework that will save cost, time, and staff required to conduct redundant agency security assessments. (GSA.gov)

Federal Information Processing Standards Publication 199 (FIPS 199): Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels. (NIST.gov)

Government Emergency Telecommunications Service (GETS): Provides National Security/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 (PSTN). 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. (NCS.gov)

Hybrid Cloud: The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. (NIST SP 800-145)

Identity Federation Framework (ID-FF): A viable approach for implementing such a single sign-on with federated identities. (Projectliberty.org)

Identity Management (IdM): 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)

ISACA: Formally the Information Systems Audit and Control Association. A nonprofit, global membership association for IT and information systems professionals. (ISACA.org)

Information Technology Markup Language (ITML): A set of specifications of protocols, message formats and best practices in the Application Service Provider (ASP) and ASP aggregation market to provide seamless integration of partners and business processes. (xml.coverpages.org/itml.htm)

Information Service: The term 'information service' means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service. (*The Communications Act*)

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. (44 U.S.C. 3502 (8))

Infrastructure: A collection of those telecommunications components, excluding equipment, that together provide the basic support for the distribution of all information within a building or campus. (Newton's Telecom Dictionary)

Infrastructure as a Service: The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145)

Interdependency: The extent to which multiple entities functioning within a single cloud or multiple clouds depend on the performance of each other to ensure stable, secure and efficient operation of the cloud environment.

Measured Service: Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service. (NIST SP 800-145)

Mission Function: A specific category of activities performed in the furtherance of NS/EP objectives.

Mobile Device Management: A tool or software that distributes applications and data to mobile devices in order to enhance the functionality and security of the device.

National Communications System (NCS): An interagency group of 24 Federal departments and agencies that coordinates and plans NS/EP telecommunications to support crises and disasters. (NCS.gov)

National Essential Functions: The subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities. (National Security Presidential Directive 51 [NSPD-51] / Homeland Security Presidential Directive 20 (HSPD-20).

National Security and Emergency Preparedness (NS/EP) Telecommunications Services: Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States. (NIST SP 800-53)

Office of the Manager, National Communications System (OMNCS): Housed within the Department of Homeland Security, the OMNCS is responsible for managing the NCS, an interagency consortium of 24 Federal departments and agencies that serves as a focal point for Government-industry national security and emergency preparedness communications planning.

On-Demand Self-Service: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service's provider. (NIST SP 800-145)

Open-ID: A tool that allows users to use an existing account to sign in to multiple websites, without needing to create new passwords. (openid.net)

Platform as a Service: The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. (NIST SP 800-145)

Policy: The set of authoritative directives related to a topic including statute, regulation, executive directions, and applicable managerial decisions, both foreign and domestic.

Primary Mission Essential Functions: Those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency. (NSPD-51/HSPD-20)

Private Cloud: The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. (NIST SP 800-145)

Public Cloud: The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. (NIST SP 800-145)

Rapid Elasticity: Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out, and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time. (NIST SP 800-145)

Resource Pooling: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines. (NIST SP 800-145)

Resiliency: The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (DHS.gov)

Risk Management: Process of identifying, controlling, and eliminating or minimizing uncertain events that might adversely affect system resources. (Newton's Telecom Dictionary)

Security Assertion Markup Language (SAML): A framework for exchanging authentication and authorization information. Security typically involves checking the credentials presented by a party for authentication and authorization. SAML standardizes the representation of these credentials in an XML format called "assertions," enhancing the interoperability between disparate applications. (NIST SP 800-95)

Service Level Agreement (SLA): An agreement between a user and a service provider, defining the nature of the service provided and establishing a set of metrics (fancy word for measurements) to be used to measure the level of service provided measured against the agreed level of service. Such service levels might include provisioning (when the service is meant to be up and running), average availability, restoration times for outages, availability, average and maximum periods of outage, average and maximum response times, latency, delivery rates (e.g., average and minimum throughput). The SLA also typically establishes trouble-reporting procedures, escalation procedures, penalties for not meeting the level of service demand – typically refunds to the user. (Newton's Telecom Dictionary)

Service Model: The manner (or model) of delivery for a given service.

Software as a Service (SaaS): The capability provided to the consumer is to use the provider's application running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure, including the network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings. (NIST SP 800-145)

Telecommunications: The transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received. (*The Communications Act*)

Telecommunications Carrier: Any provider of telecommunications services, except that such term does not include aggregators of telecommunications services (as defined in section 226[56] of this title). A telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services, except that the Commission shall determine whether the provision of fixed and mobile satellite service shall be treated as common carriage. (*The Communications Act*)

Telecommunications Service: The offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used. (*The Communications Act*)

Telecommunications Service Priority (TSP): A program that authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors frequently experience a surge in requests for new services and requirements to restore existing services. The TSP Program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service. (NCS.gov)

Terminal Device: Any device capable of sending and/or receiving information over a communications channel. The means by which data is entered into a computer system and by which the decisions of the systems are communicated to the environment it affects. (*Data Communication Technology*).

Wireless Priority Service (WPS): A method of improving connection capabilities for a limited number of authorized national security and emergency preparedness (NS/EP) cell phone users. In the event of congestion in the wireless network, an emergency call using WPS will wait in queue for the next available channel. WPS calls do not preempt calls in progress or deny the general public's use of the radio spectrum. (NCS.gov)

[56] http://www.law.cornell.edu/uscode/text/47/usc_sec_47_00000226----000-

APPENDIX D:

NS/EP CLOUD MAPPING METHODOLOGY

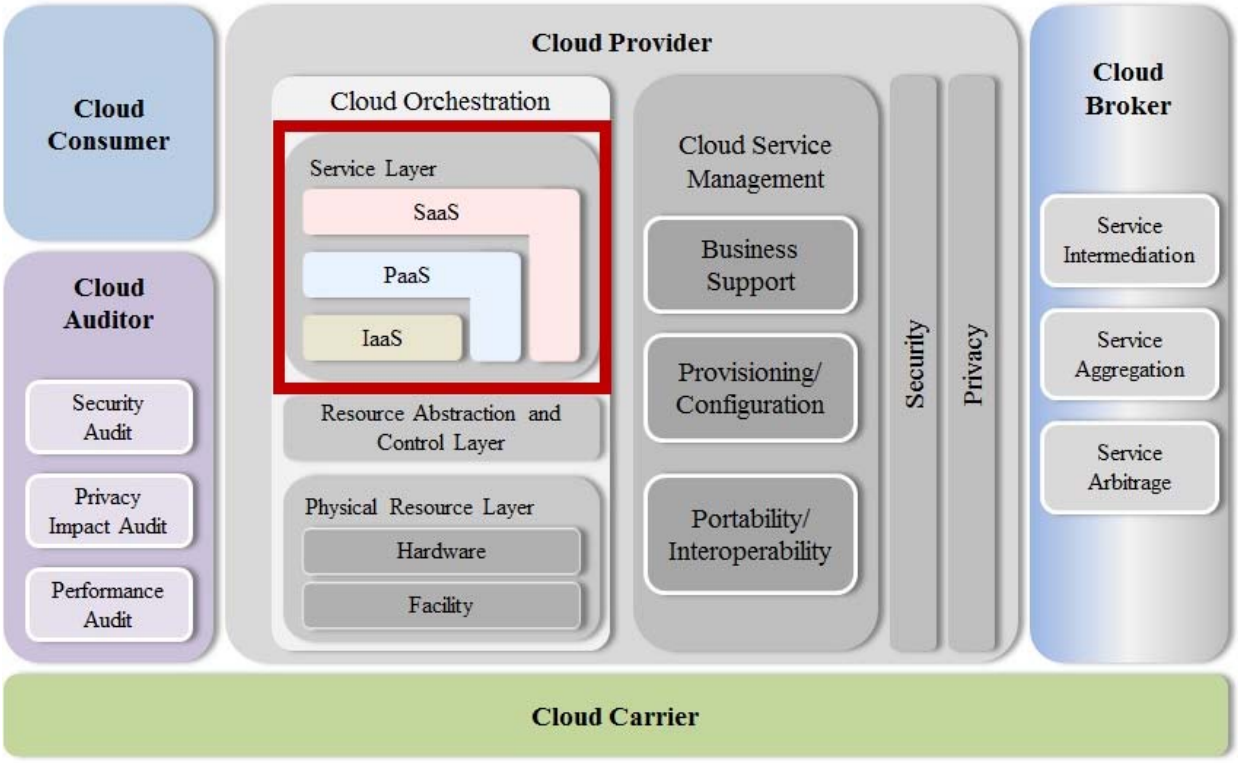
APPENDIX D: NS/EP CLOUD MAPPING METHODOLOGY

Three-Dimensional Model

There are several different approaches to examining cloud computing, which coexist as different understandings of the same subject, depending on whether one wishes to focus on how clouds are constituted, the services they may offer, or how they can be deployed. Moving from infrastructure to platform to software service offerings, the three models are progressively more inclusive in the functions performed by service providers. There is some debate regarding how these can best be portrayed and the degree of detail that can be developed within this basic understanding.

The NSTAC adopts the current National Institute of Standards and Technology (NIST) view of cloud service models within the larger service architecture, shown in Appendix D Figure 1. Therefore, the President's National Security Telecommunications Advisory Committee (NSTAC) created a three-dimensional model with the following axes: (1) the three cloud service models, defined by NIST and generally accepted in the community today; (2) the four basic cloud deployment models, defined by NIST; and (3) a set of key factors into which cloud computing can be divided. These three axes are examined in the following sections.

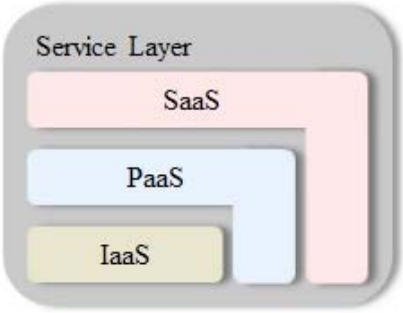
Appendix D Figure 1: NIST Service Model Architecture



Cloud Service Models

The service models associated with cloud computing are Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). **Appendix D Figure 1** portrays the progressive nature of the service model hierarchy, from least inclusive (IaaS) to most inclusive (SaaS) service offerings, while simultaneously reinforcing the notion that any of the models, standing alone, will have access to the full stack of required functions. **Appendix D Figure 2** further details this relationship, with each service model focusing on specific features and functions in its service offering while simultaneously requiring facilities, networks, hardware, or other supporting infrastructure.

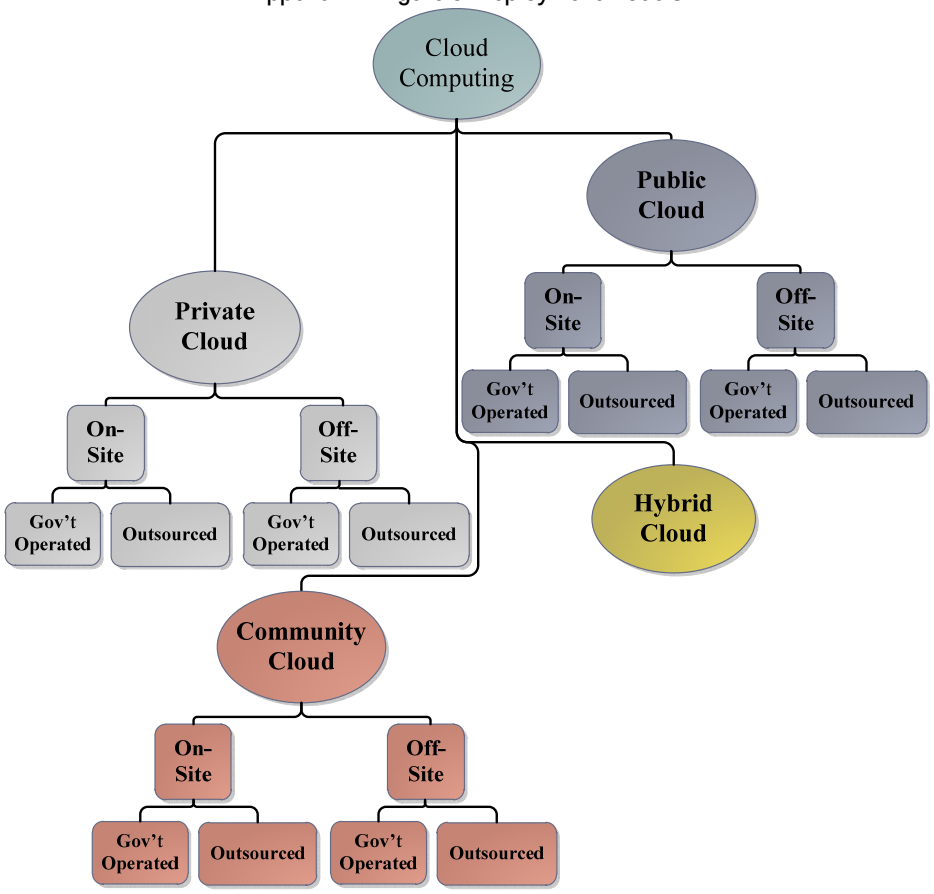
Appendix D Figure 2: Service Models



Cloud Deployment Models

Most technical authorities, including NIST, define four basic cloud deployment models: public, private, community, and hybrid. During its examination, the NSTAC found that, in the context of national security and emergency preparedness (NS/EP), it was necessary to further subdivide the four basic deployment models to fully understand the nature and extent of potential threats to cloud services. **Appendix D Figure 3** depicts the basic deployment models and defines them in terms of their hosting (either on or off-site) and whether the cloud service is Government-operated or outsourced to a commercial vendor. While not every subcategory of cloud service depicted in **Appendix D Figure 3** has been implemented, all are possible, and may be deployed in the future. Hybrid clouds, the fourth basic type of cloud computing deployment model, do not require further subdivision as they represent any combination of other cloud types.

Appendix D Figure 3: Deployment Models



Five Key Factors of Cloud Computing

As noted, the NSTAC determined that there are five key factors of cloud computing, which are defined below:

- **Data:** Recorded information, regardless of form or the media on which it may be recorded; the term includes technical data and computer software.
- **Infrastructure:** The network, processing, and storage portions of a cloud computing service, which includes the backbones, routers, switches, wireless access points, access methods, and protocols used.
- **Resiliency:** The ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies.
- **Interdependency:** The extent to which multiple entities functioning within a single cloud or multiple clouds depend on the performance of each other to ensure stable, secure and efficient operation of the cloud environment.
- **Policy:** The set of authoritative directives related to a topic including statute, regulation, executive directions, and applicable managerial decisions, both foreign and domestic.

NSTAC Cloud Computing Baseline Characteristics Matrix

To assist with its examination, the NSTAC developed a cloud computing baseline characteristic matrix (**Appendix D Figure 4**), which was intended to help identify how each of the NSTAC-identified key factor is impacted in each service and deployment model, thereby highlighting areas of study relevant to NS/EP migration to the cloud.[57] While the NSTAC initially examined various deployment models in this way, the committee determined that variances across different deployment models were not significant for the purposes of NS/EP. However, the nature and treatment of each of the five key factors varied considerable across service models.

Appendix D Figure 4: Cloud Computing Baseline Characteristics Matrix

Deployment Model	General - Applies to all Deployment Models		
Service Model[58]	IaaS	PaaS	SaaS
Characteristic[59]			
Data	Subscriber owned; normally in the custody of service provider; subscriber has broad flexibility with regard to data structure supported by the infrastructure	Subscriber owned; may be in the custody of service provider; subscriber has limited flexibility with regard to data structures supported by the platform	Subscriber owned; normally in the custody of service provider; subscriber has minimal flexibility with regard to data structures supported by the application
Infrastructure	Service provider-owned and -operated hardware	Service provider-owned and -operated hardware through middleware	Service provider owns and operates all components, infrastructure through software
Resiliency	User determined based on risk tolerance	Shared responsibility	Greatest degree of service provider responsibility
Interdependency	Lower degree of interdependency	Medium interdependency based on user on/off selection of service provider-provided features and functions	High interdependency, with detailed user selectable configuration of features and functions
Policy/Legal	Contract-based, possible jurisdictional issues. May employ strong controls by service provider	Contract-based, possible jurisdictional issues. Stronger controls by service provider	Contract-based, possible jurisdictional issues. Strongest policy controls by service provider

Cloud Computing Controls

Cloud service providers, consumers, and policy authorities can mitigate risks by establishing and diligently using proper security controls. **Appendix D Figure 5** is a sample of controls deemed

[57] Additional information can be found in the Cloud Computing Scoping Document contained in Appendix H.
[58] NIST service model and deployment model definitions can be found in the NIST SP 800-145.
[59] Characteristics are evaluated from the perspective of the subscriber.

relevant to cloud computing in the context of the key factors discussed in section X.[60] To develop this list of controls, the NSTAC examined frameworks developed by selected cloud computing organizations, including the Cloud Security Alliance (CSA), ISACA (formally the Information Systems Audit and Controls Association), the Federal Risk and Authorization Management Program (FedRAMP) policy guidelines, and the European Network and Information Security Association (ENISA). The NSTAC also examined the characteristics of various cloud models and types in the context of the NS/EP and telecommunications definitions provided in the Code of Federal Regulations Title 47, Section § 201.2, as previously discussed.

Appendix D Figure 5: Example of Cloud Computing Controls from Appendix E

Primary NSTAC Concerns	Control Specification	Responsible Party			Control Area	Unique characteristic or risk	Potential NS/EP Owner Implications
		User	Owner	Provider			
Inter-dependency	AI7.3 Implementation Plan Establish an implementation and fallback /back out plan. Obtain approval from relevant parties.		X	X	AI7 Install and Accredit Solutions and Changes New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed-upon expectations and outcomes	The process for installing and accrediting solutions may vary based on the technology, application, accreditor, organizational processes, and possibly even regulatory requirements. The length of time required can also vary and often times lag.	Cycles for updates to applications (and cloud services) are continuous, which raises concerns about the level of 3rd party access to the data and how to protect it. An NS/EP situation may not allow time for the testing of changes/ remediation of errors before implementation into the operational environment. This can reduce device/ application performance to suboptimal levels.
Infrastructure	AI7.5 System and Data Conversion Plan data conversion and infrastructure migration as part of the organization's development methods, including audit trails, rollbacks and fallbacks.		X	X			

[60] Full NS/EP control matrices are found at Appendix E.

APPENDIX E:

CLOUD COMPUTING SECURITY CONTROLS FOR NS/EP

APPENDIX E: CLOUD COMPUTING SECURITY CONTROLS FOR NS/EP

This appendix is published separately. It represents the analysis of the four security frameworks examined by the President's National Security Telecommunications Advisory Committee, including:

- Cloud Security Alliance *Cloud Controls Matrix;*
- ISACA (formally the Information Systems Audit and Control Association) *IT Control Objective for Cloud Computing: Controls and Assurance in the Cloud;*
- European Network and Information Security Agency *Cloud Computing: Benefits, Risks and Recommendations for Information Security;* and
- Federal Risk and Authorization Management Program Security Controls Baseline.

The intent is for this appendix to represent consolidated security controls tailored and specific to national security and emergency preparedness (NS/EP) requirements for implementation by NS/EP service owners under the direction of the National Communications System.

APPENDIX F

STATUTORY AND REGULATORY NS/EP DEFINITIONS

APPENDIX F: STATUTORY AND REGULATORY NS/EP DEFINITIONS

Source	Definition
Information Service 47 U.S.C. Sections 153 (24):	The term 'information service' means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.
Information System 44 U.S.C. 3502 (8)	The term information system means a discrete set of information [44 U.S.C. 3502 (8)] resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information
Emergency Preparedness System NSPD 51/HSPD 20	There is no authoritative definition for emergency preparedness systems, however systems considered relevant to emergency preparedness include systems supporting: (h) National Essential Functions (NEF) means that subset of Government Functions that are necessary to lead and sustain the Nation during a catastrophic emergency and that, therefore, must be supported through COOP and COG capabilities; and (i) Primary Mission Essential Functions (PMEF) means those Government Functions that must be performed in order to support or implement the performance of NEFs before, during, and in the aftermath of an emergency.
National Security System 44 U.S.C. 3542(b)(2)	''(a) IN GENERAL.—Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter. ''(b) ADDITIONAL DEFINITIONS.—As used in this subchapter: ''(1) The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— ''(A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; ''(B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and ''(C) availability, which means ensuring timely and reliable access to and use of information. ''(2)(A) The term 'national security system' means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency— ''(i) the function, operation, or use of which— ''(I) involves intelligence activities; ''(II) involves cryptologic activities related to national security; ''(III) involves command and control of military forces; ''(IV) involves equipment that is an integral part of a weapon or weapons system; or ''(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or ''(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. ''(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). ''(3) The term 'information technology' has the meaning given that term in section 11101 of title 40.

APPENDIX G:

NS/EP SLAS FROM NETWORX CONTRACT

APPENDIX G: NS/EP SLAS FROM NETWORX CONTRACT

National Security and Emergency Preparedness (NS/EP)[61]

Telecommunications requirements for NS/EP are based on a set of telecommunications policies and procedures established by the National Communications System (NCS) in accordance with Executive Order 12472, National Communications System, developed to ensure critical Government and industry needs are met when an actual or potential emergency threatens the security or socio-economic structure of the United States.

A national emergency is any circumstance or crisis (local, national, or international) that causes, or could cause, injury or harm to the population, damage to or loss of property, or that degrades or threatens the NS/EP posture of the United States under conditions of natural and man-made disasters and emergencies. Within the context of telecommunications services, emergency preparedness is the maintenance of a telecommunications capability in a state of readiness to meet the needs of Government (state, local, tribal, and Federal) during national emergencies.

To meet the NS/EP telecommunications requirements, the NCS administers the Telecommunications Service Priority (TSP), Telecommunications Electric Service Priority (TESP), Government Emergency Telecommunications Service (GETS), and Wireless Priority Service (WPS). [62,63]

Executive Order 12472 states that GSA "shall ensure that federally owned or managed domestic communications facilities and services meet the national security and emergency preparedness requirements of the Federal civilian departments, Agencies, and entities." Therefore, the Networx program will adhere to NS/EP guidelines and requirements.

As a critical component of the national telecommunications infrastructure, the Networx program will interoperate with, utilize, and complement the NCS NS/EP programs. Because the Networx service extends into thousands of Government offices throughout the country, the Networx networks represent a key resource for coping with emergency and disaster situations, and the Networx networks are required to be maintained in a state of readiness for any emergencies.

[61] The following section is extracted from Section C of the GSA Networx Universal contract. http://www.gsa.gov/portal/content/101611

[62] NCS administers TESP program, which promotes (on a voluntary basis) the inclusion of critical telecommunications facilities in electric service providers priority restoration plans. [http://www.ncs.gov and Footnote 61 above]

[63] FCC Network Reliability and Interoperability Council (NRIC), Homeland Security, Physical Security, NCS administered Priority Services (NRIC VI-1A-08) [http://www.nric.org/fg/nricvifg.html]

The following definitions are used in this section:

- The term Contractor's Networx network includes all infrastructures, service delivery point (SDP) to SDP, used by the contractor to provide Networx services, whether or not that infrastructure is owned by the contractor.
- Critical users of NS/EP telecommunications are key Government officials whose position requires special access and network treatment to assure telecommunications services during emergencies. During an emergency, critical users at Federal Agencies generally interact with the management of critical industries, other Federal Agencies, and state, local, and tribal Governments, on both an individual and regional basis, for developing emergency response options. It is estimated that the number of Networx NS/EP critical users will not exceed 10,000 and, for the purposes of traffic analyses, it may be assumed that they are distributed uniformly among the Networx users. The list of Networx NS/EP critical users is independent of the list maintained by the NCS, although the lists may overlap.

The following documents provide backgrounds and standards as applicable:

1. NCS "Technical Information Bulletin 02-1, February 2002"
2. NCS "National Communications System: 1963-1998, April 1998"
3. CTF "Report of the Convergence Task Force, December 2000"
4. ANSI T1.TR.79-2003, "Overview of Standards in Support of Emergency Telecommunication Service (ETS)"
5. ITU-TSS E.106, "Description of an International Emergency Preference Scheme"
6. ITU-TSS Draft F.706, "Service Description for an International Emergency Multimedia Service (IEMS)"
7. ANSI T1.631-1993 (R 1999) and Telcordia GR-2931-Core, "High Probability of Completion (HPC) Network Capability"
8. NCS "WPS FOC Requirements for GSM-Based Systems, September 2002"
9. NCS "WPS Industry Requirements for FOC for CDMA-Based Systems – Home Locations Registers (HLR), Issue 1.0; June 4, 2004"
10. NCS "GETS Legacy Functional Requirements Specification, August 2003"
11. 3GPP: 3rd generation mobile multimedia standards
12. IETF RFC 3131, IETF standardization collaboration for 3GPP
13. FCC "The Network Reliability and Interoperability Council (NRIC), Focus Group 1A, Physical Security Recommendations (specifically VI-IA-05 through VI-IA-10)", March 5, 2003
14. ANSI T1A1, ATIS TMOC and ITU standards on Emergency Telecommunications Service (ETS)

15. All new versions, amendments, and modifications to the above documents and standards as they become applicable.

Networx NS/EP Technical Requirements

Basic Functional Requirements

The following 14 basic functional requirements for NS/EP telecommunications and IT services are identified by the NCS and the Office of Science and Technology Policy for NS/EP telecommunications services and are now being endorsed by ANSI T1 and ITUTSS standard bodies and widely supported by vendor communities:

- Enhanced Priority Treatment: Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
- Secure Networks: Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
- Non-Traceability: Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
- Restorability: Should a service disruption occur, voice and data services must be capable of being reprovisioned, repaired, or restored to required service levels on a priority basis.
- International Connectivity: Voice and data services must provide access to and egress from international carriers.
- Interoperability: Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.
- Mobility: The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio).
- Nationwide Coverage: Voice and data services must be readily available to support the national security leadership and inter- and intra- Agency emergency operations, wherever they are located.
- Survivability/Endurability: Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
- Voice Band Service: The service must provide voice band service in support of presidential communications.
- Broadband Service: The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).
- Scaleable Bandwidth: NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.

- Affordability: The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
- Reliability/Availability: Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

Networx Services for NS/EP

The following Networx services, at a minimum, shall be supported during emergencies:

- Voice Services (VS)
- Cellular/Personal Communications Service (CPCS)
- Toll-Free Service (TFS)
- Audio Conference Service (ACS) [see Contract Section C.2.8.2]
- Video Teleconferencing Service (VTS)
- Frame Relay Service
- Internet Protocol Service (IPS)
- Network Based IP VPN Service (NBIP-VPNS)
- Premises Based IP VPN Service (PBIP-VPNS)
- Asynchronous Transfer Mode Service
- Secured Managed E-Mail Service (SMEMS)
- Private Line Service (PLS) [see Section C.2.5.1]
- Ethernet Service (EthS)
- Layer 2 VPN Service (L2VPNS)
- Internet Protocol Telephony Service (IPTelS)
- Voice over Internet Protocol Transport Services (VOIPTS)
- Converged IP Services (CIPS)

The Contractor shall support 14 basic functional requirements for the above Networx services as specified in Section C.5.2.2.1.1, as follows:

- VS, TFS, ACS, FRS, IPS, NBIP-VPNS, ATMS, and CPCS on contract award because commercial feasibility is already available; and [64]

[64] GSA FTS Office of Information Assurance and Critical Infrastructure Protection, "NS/EP Telecommunications Applications, July 2002"

- For the rest of the services (i.e., VTS, PBIP-VPNS, SMEMS, PLS, ES, L2VPNS, IPTelS, VOIPTS, and CIPS) after ANSI T1 and ITU standards are formally approved and commercial feasibility is developed.

The contractor shall provide an NS/EP Functional Requirements Implementation Plan (NS/EP FRIP) at Notice to Proceed. Part A of the NS/EP FRIP shall include technical systems, administration, management, and operational areas in the contract addressing how the 14 basic functional requirements will be supported for the above services. Part B of the NS/EP FRIP addresses assured service in the National Capital Region. The contractor shall revise the complete plan as required by the Networx PMO not later than 15 business days after notification by the Government.

The complete NS/EP FRIP shall be updated at least annually and provided to the Networx PMO for approval.

Appendix G Table 1: NS/EP Basic Functional Requirements Matrix for Networx Services

	NS/EP Basic Functional Requirements													
	Req #1	**Req #2**	**Req #3**	**Req #4**	**Req #5**	**Req #6**	**Req #7**	**Req #8**	**Req #9**	**Req #10**	**Req #11**	**Req #12**	**Req #13**	**Req #14**
VS	x	x	x	x	x	x	x	x	x	x			x	x
CPCS	x	x	x	x	x	x	x	x	x	x			x	x
TFS	x	x	x	x			x	x	x				x	x
ACS	x	x	x	x	x	x	x	x	x				x	x
VTS	x	x	x	x	x	x	x	x	x		x		x	x
FRS	x	x	x	x		x	x	x	x		x	x	x	x
IPS	x	x	x	x	x	x	x	x	x		x	x	x	x
NBIP_VP NS	x	x	x	x		x	x	x	x		x	x	x	x
PBIP-VPNS	x	x	x	x		x	x	x	x		x	x	x	x
ATMS	x	x	x	x		x	x	x	x		x	x	x	x
SMES	x	x	x	x	x	x		x	x				x	x
PLS	x	x	x	x	x	x	x	x	x		x		x	x
EthS	x	x	x	x		x	x	x	x		x	x	x	x
L2VPNS	x	x	x	x		x	x	x	x		x	x	x	x
IPTelS	x	x	x	x	x	x	x	x	x				x	x
VOIPTS	x	x	x	x		x	x	x	x				x	x
CIPS	x	x	x	x		x	x	x	x		x	x	x	x

Relationship with the NCS NS/EP Programs

The contractor's Networx network during NS/EP events shall interoperate with, utilize, and complement the NCS NS/EP initiatives and programs as follows:

1. **Interoperate:** The functional requirements (i.e., recognize dialing sequence and handover the call) for interoperability with the NCS GETS and WPS for end-to-end call completion during network congestions in the wireline and/or wireless networks during times of stress are described below.

   a. **NCS GETS:** The GETS provides authorized government and industry NS/EP users with a nationwide switched voice and voice band data communications priority service during periods of network congestion. The GETS universal access number is 710-NCS-GETS (710-627-4387).

      Therefore, the Networx contractor shall recognize the GETS dialing sequence and hand-over the GETS calls to NCS-identified GETS Local Exchange Carriers (LEC) for priority call processing. The contractor shall employ best effort for high probability of completion while handing over the call to the PSN.

   b. **NCS WPS:** The WPS provides authorized government and industry NS/EP users the ability to complete the call during periods of wireless networks congestion. The WPS provides end-to-end solution, fully integrated with GETS, for nationwide coverage. The WPS universal access code prefix is "*272", which needs to be dialed before the destination number (e.g., *272 703 555-1234) for priority call processing. If landline networks are also congested, dial "*272" plus the GETS access number (i.e., *272 710-NCS-GETS) to get priority in both wireless and landline networks.

      Therefore, the Networx infrastructure shall recognize the WPS dialing sequence and shall treat WPS calls as follows:

      – If the Networx contractor currently supports WPS, the contractor shall recognize the WPS dialing sequence and handover the WPS calls logically to the commercial (i.e., PSN) arm of the contractor's cellular service for priority call processing.

      – If the Networx contractor does not currently support WPS, the contractor shall treat the WPS dialing sequence as invalid and shall return appropriate announcement to the user. However, if in the future, the contractor supports WPS, the contractor shall treat WPS calls as above, from that time onward.

2. **Utilize:** The contractor shall have reserve and emergency power as per best commercial practices and whenever possible shall utilize NCS TESP for priority restoration of electric power in all transmission, switching, signaling, and major facility nodes.

3. **Complement:** After contract award, the Networx contractor shall participate, upon Government request and on an individual case basis, in studies to determine appropriate ways in which Networx network assets, and especially the many Networx dedicated access lines, may be used to support GETS.

Telecommunication Service Priority

The TSP System (FCC 88-341) provides a framework for telecommunications services vendors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunication services. The TSP System applies to common carriers, to Government, and

to private systems that interconnect with commercially provided services or facilities. The TSP System is intended to apply to all aspects of end-to-end NS/EP telecommunication services. The TSP system allows five levels of priorities for restoration and provisioning.

The contractor shall fully comply with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level for design change of circuits, including coordination between local access providers and the transport segment. The contractor shall also fully comply with any future TSP replacement system.

Should the contractor's network experience significant degradation or failure, the contractor shall provide priority restoration of affected Networx services in accordance with the TSP system five levels of priorities. In addition, the contractor shall ensure that the restored circuits retain the property of the original circuits (i.e., TSP levels). [Note that the contractor is only obligated for priority restoration and provisioning of those circuits that Agencies have obtained TSP priorities from NCS.]

Protection of SS7 Signaling System and Satellite Command Link

Protection of SS7 Signaling System: The contractor shall protect common channel signaling (ITU-TSS No. 7 or SS7) paths by using either encryption equipment endorsed under the National Security Agency (NSA) Commercial COMSEC Endorsement Program (CCEP) or any other National Institute of Standards and Technology (NIST)/NSA approved encrypted/non-encrypted forms of protection or by using other equally effective methods, such as physical isolation, message throttling, screening, and tunneling.

Protection of Satellite Command Link: If satellite communications are used in providing any Networx services (see Section C.5.2.2), the contractor shall encrypt the command and control link to any satellite launched after June 17, 1990, (in accordance with the National Telecommunications Interagency Security Subcommittee, No. 1). However, if there are other measures available that can mitigate command-link takeover, they shall be utilized wherever economical and approved on a prior basis by the Government.

Protection of Classified and Sensitive Information

The NS/EP related information includes, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and, customer profiles. In addition, the contractor will be provided access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. That information will be in various forms, including hardcopy and electronic media. It will be identified as to its classification and shall be protected by the contractor in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA approved standards as applicable for Safeguarding Classified Information). The level of classification will be up to and including Top Secret, and will be identified by the Government.

Assured Service in the National Capital Region

Because of the high concentration of traffic into and out of the National Capital Region, the contractor shall use at least two geographically separate network switches/routers to serve the National Capital Region and the loss of one of these switches/routers shall not result in a loss of more than 15 percent of total network traffic In addition, the contractor shall assure the service-specific performance levels when the PSN in the US is in severe overload condition. However, appropriate adjustments in the requirements will be made in areas where network damage has occurred.

If the National Capital Region is covered in the contract, the contractor shall:

1. Provide Part B of the NS/EP FRIP addressing the strategy for assured service in the National Capital Region
2. The NS/EP FRIP Part B shall address technical systems and administration, management, and operations requirements for the National Capital Region.

Network Evolution

The contractor shall identify to the Networx PMO the emerging technical standards for emergencies as being developed and approved by ANSI T1, ITU-TSS, and 3GPP that may impact the interoperability and reliability of any network element inserted into the mix of technologies due to technology refreshment.

NS/EP Management Requirements (Interface with the Contractor)
The Disaster Recovery Officer, as defined in Section 3.3, shall also serve as the NS/EP Emergency Liaison Officer. This requirement shall also apply to any contractor personnel designated as the liaison officer after contract award if deemed necessary by the Networx PMO. The liaison officer's top priority will be the coordination of the contractor's corporate capabilities with the Networx PMO.

APPENDIX H:

NSTAC CLOUD COMPUTING SCOPING DOCUMENT

APPENDIX H: NSTAC CLOUD COMPUTING SCOPING DOCUMENT

NSTAC CLOUD COMPUTING SCOPING GROUP

I. Overview and Background:

In December 2010, the Federal Government established a requirement that, to the extent possible, Federal agencies should migrate existing information technology services to a network-based architecture, commonly referred to as "cloud computing." To support this requirement, the Office of the Federal Chief Information Officer (OCIO) published the *Federal Cloud Computing Strategy* outlining the Federal Government's migration to cloud computing in February 2011. At the same time, many commercial entities are adopting or considering adoption of cloud computing. Commercial migration to the cloud may in some cases occur in direct support of Federal programs, but, in most cases, migration will occur for commercial purposes regardless of Federal programs.

Given the current Federal policy direction noted above, as well as the commercial sector's embrace of cloud computing, a key question surrounds the national security and emergency preparedness (NS/EP) communications considerations resulting from such migrations. In February 2011, the Designated Federal Official (DFO) for the President's National Security Telecommunications Advisory Committee (NSTAC) appointed a Cloud Computing Scoping Subcommittee (CCSS) to examine the NS/EP implications of the trend towards government use of cloud computing and to develop appropriate recommendations for deliberation by the NSTAC members, including creation of a subcommittee to investigate the implications as scoped.

II. Estimated Time Frame and Priority:

High Priority.
The estimated time frame for a subcommittee to perform work as scoped herein is six months. The subcommittee would plan to complete the final report by the end of 2011.

III. Value in Researching Issue:

Cloud adoption by both Government and industry is expected to accelerate rapidly in the near future. However, cloud computing is a relatively new concept that has not been studied rigorously or broadly surveyed from a risk perspective. Unless and until NS/EP considerations for cloud computing are studied in a focused and informed way, important questions related to those aspects of cloud migration will remain unanswered. To that extent, migration to cloud computing could create potential and even unknown risks to critical NS/EP processes and equities in both Government and industry.

Security related to cloud computing is generally presented and discussed in indistinct terms. The heart of the problem is that examinations of security posture focus on the existence of definable and measureable logical and physical system boundaries to support security assessments and management. Deeper understanding of the security issue as it relates to cloud computing will resonate beneficially in many contemplated cloud deployments.

Of note, schedule requirements in this case are such that it will be necessary to select specific, key questions for focused attention, while possibly leaving others to be addressed later. The full subcommittee's goal must be to create a broad understanding to support identification of the full scope of interest and to inform follow-on studies by the NSTAC or perhaps other entities in the future. Within that context, the NSTAC should examine and provide possible recommendations on a short list of the most immediate and pressing issues related to cloud computing and the implications for NS/EP.

Specific questions the subcommittee will focus on are:

(1) Within the context of NS/EP, what should be put in the cloud? What are the sorting/defining NS/EP considerations to determine applicability and value for migration of any given equity to a cloud computing environment?

(2) For equities that do migrate to the cloud, should the requirements for providers supporting NS/EP standards and capabilities be different than the requirements established for commercial cloud providers in general? If so, how?

(3) What will be the effects of expanded migration to and adoption of cloud services on NS/EP-relevant capabilities and programs, both present and anticipated, in terms of threat, security, stability, interdependency, resiliency, and other definable attributes?

(4) How are special considerations of multi-tenancy accommodated in NS/EP, in terms of security, privacy, and identity, etc? What NS/EP capabilities are expected to be created, altered or eliminated as a result of cloud migration?

(5) What effect will the mix of public/private/community/hybrid cloud infrastructures and architectures have on NS/EP communications? What special consideration should be given to interworking between varying cloud deployment models, service models, and legacy environments?

(6) How should NS/EP services be prioritized when offered through the cloud? How should issues such as capacity and access prioritization for cloud services be managed during NS/EP events?

(7) To what extent should Federal guidelines be taken into consideration in commercial cloud deployments supporting NS/EP? Does or should the deployment process change when implementing a cloud service for NS/EP functions?

(8) What other policy/legal considerations exist?

IV. Dismissal Reasons:

Not applicable.

V. Approach:

(1) Receive briefings from key authorities in Government and elsewhere that bear on the problem, including extant policies, technical issues, practices, lessons learned, research and other sources that may be applicable.

(2) Develop a matrix of established cloud deployment models/service models vs. identified characteristics of any/all clouds (e.g. data, infrastructure, resiliency, as detailed in the attached outline). In so doing, create a roadmap identifying NS/EP considerations across cloud computing.

(3) Categorize identified functions in terms of a list of NS/EP attributes to be developed and weighted. From this, identify the most significant considerations in cloud migration related to NS/EP.

(4) Use those findings to inform recommendations regarding priorities for cloud migration.

(5) Develop answers to questions (1) and (2) in Section III above.

(6) Examine NS/EP-related cloud computing topics, including others in Section III and as listed on the attached outline, within available time. Provide findings/conclusions and recommendations as deemed appropriate.

VI. Proposal to NSTAC:

That the NSTAC vote to create an NSTAC Cloud Computing Subcommittee. This Subcommittee would be charged to study the subject within guidelines outlined here. Cloud computing is clearly an issue of rapidly-growing importance to telecommunications in general and NS/EP in particular; its full implications need to be better understood to guide and inform future direction of policy, technical and economic activity related to the cloud.

VII. Schedule:

- Government agreement to create an NSTAC Subcommittee for Cloud Computing – June 2011
- Appointment of subcommittee Chair and members by NSTAC DFO – June 2011
- First meeting – Late June 2011
- Identify and invite relevant outside briefers and SME's – July 2011.

These include at a minimum:

o Presidential Cybersecurity Advisor

o Intelligence community threat information

o Leading examples of organizations and projects engaged in cloud computing, in both government and industry (e.g. FedRAMP, NASA, ENISA, Cloud Security Alliance, OASIS)

- Develop draft report – By September 2011
- Discuss report findings, conclusions and recommendations – October 2011
- Present draft report to NSTAC Principals – November 2011
- Smooth report and deliver to government – December 2011

APPENDIX I:

BEST PRACTICES FOR SECURING AN ENDPOINT DEVICE

APPENDIX I: BEST PRACTICES FOR SECURING AN ENDPOINT DEVICE

- Secure network VPN;
- Secure remote access for GFE and non-GFE equipment;
- Protection against data leaks and malicious code;
- Secure, unattributable access to data and internet sites;
- Must be highly adaptable and modular. It must be integrated with an agency's government-issued CAC/PIV card, or RSA token, or thumb print recognition;
- Enhance the security of an existing SSL VPN;
- Provide an alternative to updating/patching legacy equipment by creating a Thin Client;
- Must be easy to install and use and easy to expand;
- For teleworking it must convert any remote user's PC/laptop/mobile device into a trustable device;
- Password or "shared secret" modes of authentication are not secure. All authentications must be performed through an encrypted tunnel. No data flows through that tunnel until the user's authentication is accepted and verified. In addition, each data packet that flows through the tunnel must be verified on each end; and
- Technical specifications:
  - Built-in RSA PKI digital certificates for the strongest form of authentication
  - DoD PKI / standards-based authentication supporting X.509 certificates
  - OCSP and CRL checking for authentication
  - No RADIUS or SecurID ACE server required, thereby significantly reducing total operating costs and preventing man-in-the-middle attacks
  - Must support SecureID, SmartCard (CAC/PIV) and Active Directory.
  - Must create secure connections using any network medium supported by the native Windows OS included wired, Wi-Fi, and 3G/4G.
  - Must allow simultaneous use of the native OS and secure thin client access to a remote enterprise network
  - Must have redundancy and Automatic Fail-Over for VPN Appliances and Internet connectivity to ensure maximum availability for mission-critical applications and protection against Denial of Service attacks

APPENDIX J:

BIBLIOGRAPHY

APPENDIX J: BIBLIOGRAPHY

2011 Cloud Computing Planning Guide: The Shift to Hybrid IT, Gartner, Inc., Publication G00210316, March 15, 2011.

44 U.S.C. 3542.

47 U.S.C. 153 (20).

47 U.S.C. § 226 http://www.law.cornell.edu/uscode/text/47/usc_sec_47_00000226----000-

The American Institute of Certified Public Accountants, Inc. and Canadian Institute of Chartered Accountants. *Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (Including WebTrust® and SysTrust®).* 2006.

Armbrust, Michael et al. *Above the Clouds: A Berkley View of Cloud Computing, UC Berkley Technical Report No. UCB/EECS-2009-28.* February 2009.

Badger, Lee, et al. *DRAFT Cloud Computing Synopsis and Recommendations (NIST Special Publication [SP] 800-146).* May 2011. http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

Bloomberg, Michael, et al. *FDNY Counterterrorism and Risk Management Strategy.* December 2011. http://www.nyc.gov/html/fdny/pdf/publications/FDNY_ct_strategy_2011_12.pdf

The Cloud Security Alliance. https://cloudsecurityalliance.org/

Connolly, James M. *Know the Boundaries of Collaboration*. The IT Services Site. November 28, 2011. http://www.theitservicessite.com/author.asp?section_id=1577&doc_id=236085

The Communications Act. 1934.

Cover Pages. http://xml.coverpages.org/itml.html

CSC Cloud Usage Index, study by TNS, 2011.

E-Government Act of 2002, P.L. 107-347.

The European Network and Information Security Agency. http://www.enisa.europa.eu/

Executive Office of the President. *Federal Cloud Computing Strategy*. February 2011. http://www.cio.gov/documents/federal-cloud-computing-strategy.pdf.

Federal Communications Commission Network Reliability and Interoperability Council (NRIC), Homeland Security, Physical Security, NCS administered Priority Services (NRIC VI-1A-08) http://www.nric.org/fg/nricvifg.html

The Federal Risk Authorization and Management Program. http://www.gsa.gov/portal/category/102371

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*. February 2004. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Forecast: Public Cloud Services, Worldwide and Regions, Industry Sectors, 2010-1015, 2011 Update, Gartner, Inc, Publication G00213892. June 29, 2011.

The General Services Administration FTS Office of Information Assurance and Critical Infrastructure Protection. *NS/EP Telecommunications Applications.* July 2002.

General Services Administration Networx Universal Contract. http://www.gsa.gov/portal/content/101611

Harnessing the Power of Digital Data for Science and Society. Report of the Interagency Working Group on Digital Data to the Committee on Science of the National Science and Technology Council. January 2009.

ISACA https://www.isaca.org/Pages/default.aspx

Jansen, Wayne and Timothy Grance. *Guidelines on Security and Privacy in Public Cloud Computing (NIST SP 800-144).* December 2011. http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

Martin, James and the ARBEN Group, Inc. *Data Communication Technology*, 1988.

Mell, Peter and Grance, Timothy. *A NIST Definition of Cloud Computing (NIST Special Publication 800-145).* September 2011. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

National Communications System. "Government Emergency Telecommunications Service." http://gets.ncs.gov/program_info.html

National Communications System. "Telecommunications Service Priority." http://tsp.ncs.gov/

National Communications System. "Wireless Priority Service." http://wps.ncs.gov/program_info.html

National Institute of Standards and Technology. *Guide for Applying the Risk Management Framework to Federal Information Systems (NIST SP 800-37).* February 2010. http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

National Institute of Standards and Technology. *Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53).* August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

National Technology Transfer and Advancement Act.

Newton, Harry. *Newton's Telecom Dictionary*. 25th Anniversary Edition. New York: Flatiron Publishing, 2009.

The Office of Management and Budget. Circular A-119 Revised: *Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities,* February 1998.

The Office of Management and Budget, *Fiscal Year 2009 Report to Congress on the Implementation of the Federal Information Security Management Act of 2002*. http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/FY09_FISMA.pdf

Rabasa, Angel, et al. *The Lessons of Mumbai*. Rand Corporation: Arlington, Virginia, 2009. http://www.rand.org/pubs/occasional_papers/2009/RAND_OP249.pdf

Report of the Interagency Working Group on Digital Data to the Committee on Science of the National Science and Technology Council. January 2009

Responding to the Greater Tohoku Disaster, The Role of the Internet and Cloud Computing in Economic Recovery and Renewal. Internet Economy Task Force. 2011.

Rosenberg, J. and Mateos, A. *The Cloud at Your Service,* Manning Publishing, Greenwich, CT. 2011.

Security Breach Notification Laws. National Conference of State Legislatures. http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

Trade Agreements Act of 1979, as amended.

The White House. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.* February 2012. http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

The White House. National Security Directive 42: *National Policy for the Security of National Security Telecommunications and Information Systems.* June 1990.

The White House. *National Strategy for Trusted Identities in Cyberspace*. 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

The White House *Report on the Impact of Network Convergence on NS/EP Telecommunications: Findings and Recommendations*, Information Infrastructure Protection Assurance Group (IIPAG) Convergence Working Group. February 2002.