[redacted]

A REVIEW OF SECURITY REQUIREMENTS FOR LOCAL NUMBER PORTABILITY ADMINISTRATION

September 29, 2014

Table of Contents

I. Executive Summary 2
II. Introduction 5
III. Importance of the NPACs to U.S. Critical Infrastructure 7
IV. The Evolution of Standards for Protecting Critical Infrastructure 9
V. Attack Threats and the NPACs 11
VI. Analysis of Documented Security Needs for the NPACs 14
VII. Impact on the Bidding Process 23
VIII. Conclusion 26
Appendix A | Documents Reviewed 27
Appendix B | Comparison of NIST Cybersecurity Framework to NANC Requirements for NPACs 30
Appendix C | Biographies of Contributors to Report 38

I. Executive Summary[1]

For years, Americans have had the legal right to keep their wireless and wireline telephone numbers when switching carriers, and they frequently exercise this right. Carriers must constantly keep track of this switching of carriers in order to route telephone calls correctly. They do this through the nation's seven Number Portability Administration Centers ("NPACs"), each of which is operated by a single Local Number Portability Administrator ("LNPA"). Carriers electronically consult information delivered by these NPACs before completing virtually every call and text. Therefore, NPACs are critical to the completion of all telephone calls to numbers that have ever been ported between carriers, and also to numbers that have been updated by the carriers for the purpose of network upgrades and consolidations. They are also essential to local and national law enforcement agencies, which must know on a current and historical basis which carriers are associated with telephone numbers that are subject to lawful search warrants and subpoenas. The NPACs are thus an essential part of the U.S. telecommunications system and critical infrastructure. If NPACs were compromised, telephone calls and text messages might not be completed, many search warrants and subpoenas might not be served correctly, and our system for prioritizing communications in a national emergency might not function.

The Federal Communications Commission ("FCC") is currently evaluating the North American Numbering Council's recommendation for a specified vendor to serve as the next administrator for the NPACs. Though the contract concerns the public interest, it is between private parties and not subject to federal procurement rules. The terms of the bidding process,

[1] This report was prepared on behalf of Neustar, Inc. The executives from The Chertoff Group who contributed to it include Michael Chertoff, Executive Chairman; Paul Schneider, Principal; Mark Weatherford, Principal; Adam Isles, Managing Director; Joel Brenner, Senior Advisor; and Bob Butler, Senior Advisor.

including the requirements for securing the data held by the NPACs, were developed by North American Portability Management, LLC ("NAPM"), which consists of representatives of the nation's telecommunications carriers, whose interests do not necessarily coincide with those of the public.

We have carefully examined the bid terms from a national and homeland security perspective by taking the following approach: we first assessed national and homeland security risks associated with the NPACs and then assessed the extent to which the bid terms addressed those risks.

We find the bid terms insufficient in both scope and specificity when compared with widely accepted national and international standards. These standards were recently collected and incorporated into the Cybersecurity Framework published this year by the National Institute

- There is no requirement for an overarching response plan in an emergency.
- There is no requirement for a written security plan subject to government approval.

In addition to the potential for disruption, the penetration of the Local Number Portability Enhanced Analytic Platform ("LEAP")—an online portal used by law enforcement—by an agent of a foreign intelligence service or a crime syndicate would reveal the targets of law enforcement and counterintelligence investigations. That would be a counterintelligence bonanza for adversaries of the nation and a security disaster for the United States.

The security of the U.S. telecommunications system is the responsibility of the Executive Branch, in coordination with independent agencies such as the FCC. We recommend that the risk mitigation strategy associated with this contract be set forth in written requirements that are either created or vetted by the components of the U.S.

II. Introduction

In this paper we evaluate, from a national security and homeland security perspective, the sufficiency of the security requirements included by the North American Portability Management LLC ("NAPM") in its Request for Proposal ("RFP") for one or more Local Number Portability Administrators ("LNPAs") to manage the nation's seven Number Portability Administration Centers ("NPACs"). First, we summarize the importance of the NPACs as an integral component of the U.S. Government's (and the nation's) critical infrastructure. Next, we review the significant existing and potential risks—primarily in the form of Advanced Persistent Threats in cyberspace—associated with a compromise in the security of the NPACs. Finally, we compare the NAPM security risk mitigation requirements in the RFP against the established national cybersecurity framework for critical infrastructure and assess the adequacy of the security risk mitigations contained in the RFP. In essence, we are evaluating the extent to which the RFP requirements included a process to "[i]dentify the cyber risk universe, develop internal controls, assess implementation, and monitor effects," as supported by Federal Communications Chairman ("FCC") Chair Tom Wheeler in his June 12, 2014, remarks to the American Enterprise Institute.[2] Finally, we offer our views on the overall sufficiency of the LNPA selection process

[2] FCC Chair Tom Wheeler delivered remarks on cybersecurity to the American Enterprise Institute on June 12, 2014, which are available at http://www.fcc.gov/document/chairman-wheeler-american-enterprise-institute-washington-dc. He concluded in part by offering the following observations:

> "Some common success factors are already emerging from [government-industry] dialogue: First, companies conduct thorough inventories of their exposure to various cyber risks, internally and with their partners. Second, they conduct qualitative assessments of their management of those identified exposures to cyber risk. Third, they seek data from those qualitative assessments to develop quantitative metrics pertinent to their own internal needs. Fourth, they invest to close cyber readiness gaps making conscious, measured choices to mitigate risk."
>
> "In short: Identify the cyber risk universe, develop internal controls, assess implementation, and monitor effects. This sounds a lot like how enterprise risk management has always been done across all risks. Applying it to cyber risk would seem a no-brainer."

and on the most prudent way to address identified deficiencies in order to protect national security and homeland security related to the LNPAs and the administration of the NPACs.

III. Importance of the NPACs to U.S. Critical Infrastructure

The FCC defines telephone number portability as a "consumer's ability to change service providers within the same local area and still keep the same telephone number."[3] Under FCC rules, consumers may exercise this ability for both wireline and wireless telephone numbers. As directed by the FCC, regional NPACs hold the telecommunications industry's common, authoritative databases used for routing, rating, and billing calls to ported telephone numbers and other routing information changes resulting from technology migrations or merger activities. One or more LNPAs may be appointed to manage the regional NPACs to accomplish this critical role, which includes securely delivering this critical information to service provider networks in real time. These NPACs process tens of millions of transactions every month, ensuring that the correct and most current service provider is associated with each ported telephone number. Virtually every call that terminates within North America relies on information from the NPACs to be routed to completion.[4] The authoritative routing information for over 650 million U.S. telephone numbers is stored in and distributed from the NPAC.[5] The telephone system within North America relies on the NPACs to function normally; without them, telephone calls and text messages to hundreds of millions of numbers would not function properly. This same system provides critical communications and information system support to U.S. Government law enforcement and emergency preparedness programs.[6]

---

[3] FCC, Wireless Local Number Portability (WLNP), at http://www.fcc.gov/encyclopedia/wireless-local-number-portability-wlnp; for wireline service, *see also* FCC, Portability: Keeping Your Telephone Number When You Change Service Provider, http://www.fcc.gov/guides/portability-keeping-your-phone-number-when-changing-service-providers (wireline service).

[4] *See* http://www.npac.com/number-portability/the-npac-neustar-lnp.

[5] *See* http://www.neustar.biz/thetechnology/npac/facts-and-figures.

[6] *Reply Comments of the FBI, DEA and USSS in the Matter of NANC Recommendation of a Vendor to Serve as Local Number Portability Administrator*, Docket No. CC 95-116, WC 09-109.

As stated in Presidential Decision Directive 63 in 1998, "Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private."[7] The U.S. Government has designated the telephone system and associated telecommunications systems as critical infrastructure.[8] In addition, the information systems supporting the effective operation of the telephone system and telecommunication infrastructure have also been designated as critical infrastructure.[9] Since its inception in 2003, the U.S. Department of Homeland Security ("DHS") has had the responsibility to coordinate this critical infrastructure support, and in conjunction with other U.S. Government-designated lead agencies and industry, "to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."[10] In short, because of their essential role in telecommunications, the LNPA and the management of the regional NPACs are critical to the effective operation of the U.S. telecommunications and supporting information systems infrastructure.

[7] *See* http://fas.org/irp/offdocs/pdd/pdd-63.htm.
[8] *See* http://web.archive.org/web/20130613014943/http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf.
[9] *See* http://www.dhs.gov/sites/default/files/publications/IT%20Sector%20Specific%20Plan%202010.pdf.
[10] *See* http://www.dhs.gov/homeland-security-presidential-directive-7.

IV. The Evolution of Standards for Protecting Critical Infrastructure

In February 2013, President Obama issued Executive Order 13636, entitled *Improving Critical Infrastructure Cybersecurity,* which called on the Department of Commerce's National Institute for Standards and Technology ("NIST") to develop a national cybersecurity framework to enhance the protection of U.S. critical infrastructure and services. Executive Order 13636 defines critical infrastructures as those "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[11]

NIST published the first version of its Cybersecurity Framework ("NIST Framework") in February 2014.[12] The NIST Framework compiled and endorsed a broad collection of controls, drawn from existing standards and best practices. Those existing standards include COBIT, ISO 27001, ISA/IEC-62443 ("ISA-99"), and NIST Special Publication 800-53, as well as the Council on Cybersecurity's 20 Critical Controls for Cyber Defense (hereinafter the "CSC 20"; formerly known as the "SANS 20"). The formally documented controls are mapped section-by- section to the framework in the NIST Framework document. The NIST Framework compiles and advances an existing body of knowledge, rather than attempting to abandon existing wisdom in favor of new but untested approaches.

This NIST Framework is built upon five categories of core elements for an effective technology risk mitigation strategy applicable to any enterprise: (i) identification; (ii) protection; (iii) detection; (iv) response; and (v) recovery. Using these core elements, the NIST Framework delineates a series of functional actions to achieve cybersecurity outcomes. It should be

[11] *See* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
[12] *See* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

emphasized that the NIST Framework reflects existing commercial and governmental standards that have been maturing for several years.

The NIST Framework states: "Due to the increasing pressures from external and internal threats, organizations need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk."[13] Recognizing this increasing pressure, FCC Chairman Tom Wheeler has clearly stated the need for applying and operationalizing the NIST Framework in the telecommunications infrastructure.[14] As previously stated, the NPACs play an essential role in achieving these objectives.

[13] *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, p.3.
[14] *See* http://www.fcc.gov/document/chairman-wheeler-statement-cybersecurity-framework.

V. Attack Threats and the NPACs

Cyber threats to the NPACs are real, significant, and growing. These cyber threats often involve sophisticated attacks using computer malware known as Advanced Persistent Threats ("APTs"), which are difficult to detect and remove, and social engineering attacks such as "phishing," or "spear phishing," which involve misleading communications from what appear to be trusted sources. The object of a phishing attack is to induce the unsuspecting target(s) of the communication to click on, and unknowingly install, the APT malware on its organization's system. APT attacks often come from sophisticated threat actors—ranging from nation-states to transnational terrorist organizations to criminal enterprises—and can penetrate sophisticated systems and harm critical infrastructure systems and services. These penetrations can cause physical damage as well as service disruptions.

For example, the damage resulting from the 2012 Shamoon virus attack on the Saudi Aramco energy operation highlights the physically destructive nature of today's APTs.[15] In that attack, the operating system software and all data on over 30,000 computers were totally erased and the computers rendered inoperable. The ever-increasing exploitation and disruptive attacks against U.S. financial services firms clearly indicate the intensity and sustained nature of APT attacks against critical infrastructure in the financial sector.[16] Overseas, last year's cyber-attack

[15] *See* http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf; *see also* http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all&_r=0.

[16] *See* http://www.investmentnews.com/article/20140110/FREE/140109928/cybersecurity-threats-to-financial-firms-on-the-upswing-in-2014.

against Telenor—Norway's giant telecommunications company—proved that telecommunications providers are not exempt from cyber-attack.[17]

There are at least three different APT attack scenarios against the LNPAs that demand a robust risk mitigation strategy.[18] The first is the potential for a cyber-attack resulting from the exploitation of the Local Number Portability Enhanced Analytic Platform ("LEAP"). LEAP is a "subscription-based, online portal which allows law enforcement agencies to retrieve information on numbers"[19] and allows U.S. law enforcement agencies to immediately determine telephone number assignment. This function is essential to correctly direct a subpoena or court order for records or a wiretap to the appropriate telecommunications provider. An attacker who was able to penetrate this system would be able to determine the targets of law enforcement investigations. That knowledge would permit the attacker to determine whether any of its clandestine agents in the United States were under investigation. This would be a counterintelligence bonanza for an adversary wanting to steal sensitive U.S. wiretap and law enforcement queries and, conversely, a counterintelligence and security disaster for the United States.

A second threat scenario involves potential attacks arising from the exploitation of Location Routing Number database, which serve the critical function of mapping updates to routing information. This form of attack, which misdirects calls to erroneous or nonexistent terminating networks, could affect all carriers across North America and could disrupt the telephone system for hours or even days at a time, with a severe effect on critical infrastructure

[17] ***See*** http://www.spamfighter.com/News-18262-Massive-Cyber-attack-Strikes-Telenor-Major-Telecommunications-Company-of-Norway.htm.
[18]

and on personal and business communications. A variation of this scenario would involve a focused misdirection attack on the voice communications systems of national security and homeland security officials during a national emergency. Such an attack might result in the inability of officials to receive voice communication and some types of cellular data communications, with such calls misdirected to other locations.

A third attack scenario revolves around potential attacks arising from the exploitation and control of the NPACs and their interaction with multiple carrier/operator systems. In this scenario, access might be gained by obtaining knowledge of the carrier subsystems through interconnected LNPA operational and business subsystems. Once access is obtained, malicious code could be inserted into the telecommunications infrastructure to adversely impact the supply chain. If such an attack were successful, the potential consequences could be devastating, and might

VI. Analysis of Documented Security Needs for the NPACs

In light of these plausible threats against NPAC-related critical infrastructure, we studied the documented security requirements proposed for the NPACs by the NAPM and the North American Numbering Council ("NANC"), the industry groups charged with drafting the RFP. These requirements are set forth in the Functional Requirements Specification ("FRS") and Technical Requirements Document ("TRD"). We then compared these requirements to the security controls articulated in the NIST Framework. A list of the documents we reviewed is found in Appendix A.

In the FRS and the TRD, eight (8) categories of security requirements are listed, which include:

- identification requirements,
- authentication requirements,
- access control requirements,
- data and system integrity requirements,
- audit requirements,
- continuity of service requirements,
- software vendor requirements, and
- mechanized security environment requirements.

These categories and their subordinate requirements provide broad guidance for some (but not all) of the security controls and specific guidance for a few of the security controls. Access to systems, restrictions in the use and provisioning of accounts, and protection of the

authentication chain are all detailed. Similarly detailed are a host of mechanized[20] security controls that provide a platform for detecting many common attack techniques. Most of the remaining controls are divided between establishing a foundation for supporting system availability, integrity, confidentiality, and recovery and providing some basic intrusion detection and incident response/auditing capabilities. Although the categories and delineation of requirements within these categories represent some key elements of a risk mitigation strategy, they are not a comprehensive list of requirements as defined by the NIST Framework to help mitigate external threats and risks to the NPACs. In fact, they are a rather narrow subset of the security requirements found in the NIST Framework or, indeed, in any prudent list of security requirements for protection of a critical information system. Appendix B shows a requirement-by-requirement comparison, highlighting the RFP's deficiencies in all five core NIST Framework categories of identification, protection, detection, response, and recovery.

When we compared the RFP's security requirements to the NIST Framework's functional controls, we made the following key findings.

- **Identification Core Requirements**: The FRS and TRD provide detailed data flows and require documentation of vendor communication with or access within the system—both key aspects of the NIST Framework. *However, inventory and prioritization of assets, including personnel roles, are not identified as a requirement. While such inventory may be created and maintained in the course of system administration, they should be formally required and should become part of the criteria for pre-award and post-award evaluation of the vendor. One of the most widely acknowledged sources of guidance on how to prioritize cybersecurity actions*

[20] The FRS and TRD use the term "Mechanized Security Environment" to describe a system using logical or cryptographic controls, as opposed to processes, to prevent or detect tampering.

is the Council on Cybersecurity's 20 Critical Controls for Cyber Defense ("CSC 20"). This guidance is built from the knowledge of actual cyber-attacks that have compromised systems, and it is referenced with authority in the NIST Framework. Maintaining an inventory of hardware and software assets—particularly for critical systems—is at the top of the CSC 20 list. These inventories form the foundation for ensuring that assets are securely configured—conversely, lack of inventories makes it impossible to ensure comprehensive configuration control. In addition, without valid asset inventory data, it may be impossible to achieve complete containment, response, and remediation following a security incident since remediation efforts will likely fail to account for all malicious activity hidden in non-inventoried assets. The NIST Framework identifies the awareness of the "Business Environment" and governance requirements of the system as critical to the ability to assess risk and prioritize activities. The FRS and TRD do not specifically require that this awareness be incorporated into security processes. While the FRS and TRD enumerate a small number of example threats, *there is no requirement for a complete risk assessment and risk management program to discover and monitor risk, while tracking and prioritizing its mitigation. Such a program is among the most critical aspects of maintaining a secure system, because it forms the basis for defining and updating risk response and monitoring activities. This point is a core feature of NIST Special Publication 800-39, the agency's longstanding guidance for managing information security risk.*

- **<u>Protection Core Requirements</u>**: The FRS and TRD outline key requirements for the management of identities and credentials. However, the requirements *do not adequately detail restrictions for vendor access to systems or delineate between "user" and "personnel" roles.* The FRS and TRD adequately require capacity planning to address certain kinds of denial of service, and they contain the foundation for much of the remainder of what NIST refers to as "Data Security" controls. But while encryption standards are defined, *they are required only for a subset of data of likely insufficient scope. Likewise, expansion of existing controls and the addition of requirements concerning asset lifecycle management, data leakage, and testing/development are highlighted as key needs in the NIST Framework. The FRS and TRD identify a requirement that software be developed using a lifecycle methodology, but neither document speaks to the need for information security to be formally factored into a system lifecycle management methodology to provide more holistic protection, including configuration control, data destruction, and continuous improvement. In the spirit of "an ounce of prevention is worth a pound of cure," integrating security planning into the system development lifecycle ("SDLC") early, e.g., at the requirements identification phase, can both (a) reduce the cost and complexity of building security into a system after the fact, and (b) align security and underlying business processes up front to make for a more seamless user experience. A thorough risk assessment should occur at the beginning of the system development process and should inform security requirements, a principle embodied in NIST Special Publication 800-64, Security Considerations in the System Development Lifecycle. Moreover, the NIST Cybersecurity Framework provision on SDLC*

references numerous developer configuration, testing and evaluation, and supply chain controls and related tools provided for in NIST Special Publication 800-53, the agency's core security and privacy controls guidance document. These controls and tools include such items as firmware integrity verification, hardware integrity verification, version control integrity, manual code review, dynamic code analysis, threat modeling, attack surface reduction, penetration testing, and supply chain traceability.

- *A well-known potential vector for malicious code insertion is to compromise the supply chain. That is easier to do if code is written overseas or in the United States by untrusted persons. However, the NAPM has not formally required that the software in the NPACs be written by persons who have undergone background checks. Indeed, the requirements in general appear to contain no security-related personnel management provisions. Addressing cybersecurity risk in personnel screening is also an attribute of the NIST Framework and supporting controls. Likewise, FCC orders authorizing the transfer of telecommunications licenses to foreign-owned acquirers (in friendly countries) have repeatedly been conditioned on corporate security offices being located within the United States and staffed by assigned U.S. citizens. No such requirements are reflected in the FRS or TRD. In our view, these omissions are not prudent and could compromise national security notwithstanding a minimally compliant bid.*
- *NIST Framework-identified security best practices emphasize the importance of requiring standard secure baseline Information Technology configurations for devices, operating systems, and applications. The FRS and TRD are totally silent on*

secure configuration control. Default operating system and application configurations (e.g., open ports, default passwords, unneeded software) are often set for ease of implementation rather than security, and an adversary can easily exploit the resulting gaps to access the network or move laterally within the network. It is thus critical to (a) employ a baseline security configuration that addresses such issues and (b) continuously manage such configurations to prevent "security decay" as baseline configurations are modified, for example, to support new software installation.[21] *The CSC 20 cites the use of hardened images as a key control. Further, the NIST Framework highlights the need for regular identification and patching of vulnerabilities. Neither the FRS nor the TRD contains any formal vulnerability scanning or patching requirement. Attackers are adept at exploiting poor network hygiene—e.g., known configuration and software vulnerabilities that remain unpatched—to move laterally within a network. The past few years have witnessed a steady decline in the time between the discovery and announcement of a new vulnerability and the appearance of exploits built on that vulnerability. This puts a premium on effective and timely configuration and patch management. According to NIST: "Since the late 1990's, the length of time between the announcement of a new major vulnerability and the release of a new exploit has dropped from months to weeks or days."*[22] *The CSC 20 identifies timely patching as among the top five most urgent controls.*

[21] *See* CSC Critical Security Control 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers, *available at* http://www.sans.org/critical-security-controls/control/3.
[22] *See* NIST Special Publication 800-40, Creating a Patch and Vulnerability Management Program (p. 1-2), *available at* http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf.

- *The NIST Framework also calls for backups to be kept, but there is no explicit requirement to test the back-ups. Even where requirements are reasonably detailed, there is no requirement to actually test the system's recovery from an event.* Maintenance and repair performance and methods, however, are reasonably well outlined. *What NIST calls "Protective Technology" is similar to what the NAPM calls "Mechanized Security."* Requirements for logging, maintaining, and auditing logs are robust*, but should be applied to more of the system components, including removable media.*

- **Detection Core Requirements**: The FRS and TRD requirements establish an adequate auditing capability to detect, aggregate, correlate, and analyze events that are captured. *The documents, however, lack a requirement for establishing severity thresholds as an integral component of an overall risk program as well as the explicit establishment of alert thresholds for action. These thresholds and related response plans need not be identified in the FRS or TRD, but their establishment and maintenance should be mandated.* Existing requirements speak to monitoring of personnel and account activity for indications of illicit use*; however, the requirements must be expanded or new requirements added that incorporate similar incident detection and monitoring of network traffic, physical environment, malicious code, mobile code, and vulnerability scanning. There are no requirements that speak to personnel roles in detection, testing, improvement of capabilities, and communication.*

- *Moreover, real security requires more than compliance with a checklist—to be trusted, security functionality must be continuously assessed for implementation, effectiveness, and impact through risk-monitoring capabilities. Many well-known network breaches have involved systems that were at least superficially compliant with applicable standards in their industries. Security is an ongoing challenge that requires constant, real-time monitoring of system conditions, including regular third-party red-teaming against constantly changing threat tactics. This is the only sure way to deal effectively with the adaptive nature of the APTs likely facing the NPACs and LNPAs. It also requires imposing good practices on users that must be automatically enforced.*

- **Response Core Requirements**: *The FRS and TRD omit a requirement for an overarching Incident Response ("IR") plan. Triage capabilities should be required and mandated to start from the beginning of an event which would ensure that adequate consideration is provided to all events as potential security incidents. The FRS and TRD need not specify lines of communication during response activity but should require the awarded vendor to coordinate an IR plan that encompasses role definition, reporting, information sharing, and coordination with stakeholders, whether they are internal or external to the organization*. Auditing and response to detected events are adequately mandated in the FRS and TRD*; however, those requirements should be expanded to include impact analysis, forensics, and incident categorization. While mitigating cyber intrusions is an arms race against attackers, the FRS and TRD should require vendors to demonstrate an ability to competently*

mitigate common attack vectors or techniques. The objective of the requirement is to increase the chances of containing, mitigating, or identifying threats to the subject system or interconnected systems.

- **Recovery Core Requirements**: The FRS and TRD require the development of recovery procedures but *should also include a requirement that the vendor develop a triage plan that can be practically executed at the onset of a detected event. The FRS and TRD should further require the plan to include a maturity process that improves the system itself by incorporating lessons learned. The requirements should also dictate to the vendor proper public and internal communication, taking into consideration the need to safeguard reputation during and after recovery activities.*

VII. Impact on the Bidding Process

The FCC's decision on how to proceed to incorporate better security requirements will have much to do with the level of security it actually achieves. We have thus far focused on comparing the NAPM's security requirements with the more robust security controls that are widely accepted by security professionals, and we have found the NAPM's requirements lacking. This next question is what to do about it. In answering this question, several key principles apply:

- In our experience, where requirements are deemed essential to the effective functioning of the system, acquisition best practice dictates that they be stated with specificity. International standards on requirements engineering provide that, for requirements to be well-formed, they must be "complete." In other words, "[t]he set of requirements needs no further amplification because it contains everything pertinent to the definition of the system or system element being specified."[23] Technology modernization best practices also provide that it "is important to eliminate or at least reduce ambiguities [in requirements] as early as possible because the cost of them increases as we progress in the development life cycle."[24] As described above, that was not the case in this RFP—security requirements on secure SDLC, asset inventory management, secure configuration management, and patching are completely omitted, as is any requirement for an ongoing risk management program (i.e., a continuous cycle of risk assessment, risk response, and risk monitoring). In this case, given both the sensitive law enforcement applications

[23] *See* ISO/IEC/IEEE 29148:2011(E), International Standard: Systems and software engineering — Life cycle processes — Requirements engineering.
[24] *See* Carnegie Mellon White Paper: Requirements & Specifications, Spring 1999, *available at* http://users.ece.cmu.edu/~koopman/des_s99/requirements_specs/.

entailed in LEAP and the more general APT-related risks facing the LNPAs, strong security should have been considered as an essential component of the system and thus spelled out with specificity in the requirements.

- Likewise, for requirements to be effectively articulated, all key stakeholders must be actively involved in a dialogue with program officials on requirements.[25] International standards on requirements engineering start with the following simple proposition: "Defining requirements begins with stakeholder intentions."[26] In this case, it does not appear that LEAP users—or more importantly, emergency communications and cybersecurity experts at DHS, or threat experts at ODNI—were materially involved in requirements development or in evaluation of the received proposals.
- We do not believe that the defects cited in this report can be remedied simply by post-award contract negotiation. Several remedies are available, ranging from canceling the procurement and conducting a new competition to a more limited step involving the reopening of negotiations with respect to changed requirements. We are not in a position to weigh the relative operational impact of these corrective options, but we do conclude that the current deficiencies and resulting impact on the local number portability system are serious, that failure to include contract terms widely recognized as crucial to security likely had a significant impact on offerors' proposals, and that the NAPM would also likely lose significant leverage to obtain a best value proposal

[25] *See, e.g.*, GAO Report: Leveraging Best Practices to Ensure Successful Major Acquisitions, Nov. 13, 2013, *available at* http://www.gao.gov/assets/660/658958.pdf. While the LNPAS acquisition is not a federal government acquisition, best practice principles articulated by the Government Accountability Office apply broadly.
[26] *See* ISO/IEC/IEEE 29148:2011(E), International Standard: Systems and software engineering—Life cycle processes—Requirements engineering.

if the FCC permitted it to simply address these deficiencies in a post-award negotiation.

VIII. Conclusion

Based on this review of the RFP's requirements, it is our assessment that the current security requirements for the administration of the NPACs are insufficient to protect the NPAC critical infrastructure against the sophisticated threats currently posed against the system. To better ensure risk mitigation against these threats and to more effectively comport with U.S. Government Executive Branch guidance, the FCC and the NAPM should adopt a more robust risk mitigation strategy as part of the NPAC security plan, which should be set forth in written requirements that are either created or vetted by the organizations of the U.S. Government with experience in and responsibility for cybersecurity, preferably the Executive Branch's "Team Telecom" and cybersecurity experts in DHS. The FBI and other government law enforcement authorities have plainly said that this "security plan should comply with the NIST cybersecurity framework."[27] We agree. Indeed, it should also require continuous risk management for APTs to include validation by qualified third party security assessors. Failure to take these steps would put the NPACs at significant risk, which in turn would endanger U.S. telecommunications systems and U.S. national security.

[27] *Reply Comments of the FBI, DEA and USSS in the Matter of NANC Recommendation of a Vendor to Serve as Local Portability Number Administrator,* Docket No. CC 95-11, WC 09-109.

Appendix A | Documents Reviewed

Primary Documents

North American Numbering Council (NANC) Functional Requirements Specification for the Number Portability Administration Center (NPAC) Service Management System (SMS), Release 3.4.6, April 11, 2014.

2015 LNPA Technical Requirements Document.

NIST Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014.

NIST Special Publication 800-39, *Managing Information Security Risk.*

NIST Special Publication 800-40, *Creating a Patch and Vulnerability Management Program.*

NIST Special Publication 800-53 (Rev. 4), *Security and Privacy Controls for Federal Information Systems and Organizations.*

NIST Special Publication 800-64, *Security Considerations in the System Development Lifecycle.*

NIST Special Publication 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.*

Council on Cybersecurity, *The Critical Controls for Effective Cyber Defense,* Version 5.0

FCC Memorandum Opinion and Order, *In re Applications of Voicestream Wireless Corporation, Powertel, Inc. and Deutsche Telekom AG for Consent to Transfer Control of Licenses and Authorizations Pursuant to Sections 214 and 310(d) of the Communications Act, IB Docket 00-187.*

FCC News, *Statement from FCC Chairman Tom Wheeler on the Cybersecurity Framework,* February 12, 2014.

FCC News, Remarks of *FCC Chairman Tom Wheeler to the American Enterprise Institute*, June 12, 2014.

Reply Comments of the FBI, DEA and USSS in the Matter of NANC Recommendation of a Vendor to Serve as Local Number Portability Administrator, Docket No. CC 95-116, WC 09-109.

Chain Security White Paper, *Vulnerability Analysis Regarding Local Number Porting Services in the US*, February 25, 2014.

Chain Security White Paper, *Number Portability Architectures and Associated Vulnerabilities*, April 2014.

GAO Report: Leveraging Best Practices to Ensure Successful Major Acquisitions, November 13, 2013.

ISO/IEC/IEEE 29148:2011(E), International Standard: Systems and software engineering—Life cycle processes—Requirements engineering.

We also reviewed the following documents provided by Neustar:

Reply Comments of Neustar in the Matter of Petition of Telcordia Technologies Inc. to Reform or Strike Amendment 70 to Institute Competitive Bidding for Number Portability Administration and to end the NAPPM LLC's Interim Role in Number Portability Administration Contract, August 8, 2014.

Neustar Working Paper, *National Security Must Be a Priority in Critical Infrastructure*.

Neustar Working Paper, *Number Portability: Law Enforcement Assistance and Potential Change to Foreign-based Administrations*.

Neustar Document, *Number Portability Presentation*.

White Paper, *India's Experience with Mobile Number Portability*, May 3, 2012.

Appendix B | Comparison of NIST Cybersecurity Framework to NANC Requirements for NPACs

COLOR LEGEND	
Green	The NIST requirement is addressed and references the section in the NANC documentation where the NIST requirement is addressed.
Yellow	The NIST requirement is partly addressed and remarks describe what specifically is addressed.
Red	The NIST requirement is not addressed in the documentation provided.

NIST Cybersecurity Framework Subcategory		NANC NPAC FRS 3.4.5c 04-11-14
IDENTIFY (ID)[28]	**ID.AM-1:** Physical devices and systems within the organization are inventoried	(7.5 R7-63 calls for identification of originator, but not inventory)
	ID.AM-2: Software platforms and applications within the organization are inventoried	(7.5 R7-63 calls for identification of originator, but not inventory) (7.7 R7-85.1/2 applies only to Service Management System (SMS), not components)
	ID.AM-3: Organizational communication and data flows are mapped	7.8 R7-88 (explicitly covers vendor "entry") 1 2 Appendix A
	ID.AM-4: External information systems are catalogued	(7.5 R7-64 calls only for positive identification, not catalog)
	ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	

[28] The colors in the left-hand column correspond to colors utilized in the NIST Cybersecurity Framework to differentiate each functional element.

	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	(7.4 neither identifies nor requires roles, just individual accounts)
	ID.BE-1: The organization's role in the supply chain is identified and communicated	
	ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	
	ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	
	ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
	ID.BE-5: Resilience requirements to support delivery of critical services are established	
	ID.GV-1: Organizational information security policy is established	
	ID.GV-2: Information security roles and responsibilities are coordinated and aligned with internal roles and external partners	(7.4.2 may imply but speaks primarily to preventing shared accounts)
	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
	ID.GV-4: Governance and risk management processes address cybersecurity risks	
	ID.RA-1: Asset vulnerabilities are identified and documented	
	ID.RA-2: Threat and vulnerability information is received from information-sharing forums and sources	
	ID.RA-3: Threats, both internal and external, are identified and documented	(7.9.1 lists five examples; this is not adequate to meet the intent of this control)
	ID.RA-4: Potential business impacts and	

	likelihoods are identified	
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	(7.9.1 lists five examples, this is not adequate to meet the intent of this control)
	ID.RA-6: Risk responses are identified and prioritized	
	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders	
	ID.RM-2: Organizational risk tolerance is determined and clearly expressed	
	ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis	
PROTECT (PR)	**PR.AC-1:** Identities and credentials are managed for authorized devices and users	7.2 7.4.1 7.3
	PR.AC-2: Physical access to assets is managed and protected	
	PR.AC-3: Remote access is managed	7.8 (regarding vendor)
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	7.4.2 (differentiates only between "Users" and "Number Portability Administration Center (NPAC) personnel")
	PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	
	PR.AT-1: All users are informed and trained	
	PR.AT-2: Privileged users understand roles and responsibilities	
	PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	

	PR.AT-4: Senior executives understand roles and responsibilities	
	PR.AT-5: Physical and information security personnel understand roles and responsibilities	
	PR.DS-1: Data at rest is protected	7.3.1 R7-15 (Passwords only)
	PR.DS-2: Data in transit is protected	7.3.1 R7-19 (Passwords only) 7.9.3 (speaks to authentication for Common Management Information Protocol ("CMIP") interface communication)
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	
	PR.DS-4: Adequate capacity to ensure availability is maintained	7.7 R7-82
	PR.DS-5: Protections against data leaks are implemented	
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	7.5 (Service Management System (SMS) data only, not appurtenant systems, software or firmware) 7.9.3.2 CMIP interface only)
	PR.DS-7: The development and testing environments are separate from the production environment	
	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	
	PR.IP-2: A system development life cycle to manage systems is implemented	7.8 R7-86
	PR.IP-3: Configuration change control processes are in place	

	PR.IP-4: Backups of information are conducted, maintained, and tested periodically	7.7 R7-84.2/4 (does not include testing)
	PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	
	PR.IP-6: Data is destroyed according to policy	
	PR.IP-7: Protection processes are continuously improved	
	PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	
	PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	7.7 (includes recovery only, not response)
	PR.IP-10: Response and recovery plans are tested	
	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
	PR.IP-12: A vulnerability management plan is developed and implemented	
	PR.MA-1: Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	10.1
	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	7.8
	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	7.6.1 7.6.2 7.9.3.5
	PR.PT-2: Removable media is protected and its use restricted according to policy	
	PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	
	PR.PT-4: Communications and control	7.3.1 R7-19 (passwords

	networks are protected	only) 7.9.3 (light requirements and only for some components)
DETECT (DE)	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	7.5
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	7.6.2
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	7.6.2
	DE.AE-4: Impact of events is determined	
	DE.AE-5: Incident alert thresholds are established	
	DE.CM-1: The network is monitored to detect potential cybersecurity events	7.6.2 (not especially clear but appears to be part)
	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	
	DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	7.6.2
	DE.CM-4: Malicious code is detected	
	DE.CM-5: Unauthorized mobile code is detected	
	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	7.6.2 ("external service provider" not specifically called out) 7.8 (vendor access is logged but not activity)
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	7.6.2
	DE.CM-8: Vulnerability scans are performed	
	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability	

	DE.DP-2: Detection activities comply with all applicable requirements	
	DE.DP-3: Detection processes are tested	
	DE.DP-4: Event detection information is communicated to appropriate parties	
	DE.DP-5: Detection processes are continuously improved	
RESPOND (RS)	**RS.RP-1:** Response plan is executed during or after an event	
	RS.CO-1: Personnel know their roles and order of operations when a response is needed	
	RS.CO-2: Events are reported consistent with established criteria	
	RS.CO-3: Information is shared consistent with response plans	
	RS.CO-4: Coordination with stakeholders occurs consistent with response plans	
	RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	
	RS.AN-1: Notifications from detection systems are investigated	7.6.2
	RS.AN-2: The impact of the incident is understood	
	RS.AN-3: Forensics are performed	
	RS.AN-4: Incidents are categorized consistent with response plans	
	RS.MI-1: Incidents are contained	
	RS.MI-2: Incidents are mitigated	
	RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	
	RS.IM-1: Response plans incorporate lessons	

	learned	
	RS.IM-2: Response strategies are updated	
RECOVER (RC)	**RC.RP-1:** Recovery plan is executed during or after an event	(7.7 outlines procedures but does not mandate execution)
	RC.IM-1: Recovery plans incorporate lessons learned	
	RC.IM-2: Recovery strategies are updated	
	RC.CO-1: Public relations are managed	
	RC.CO-2: Reputation after an event is repaired	
	RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	

Appendix C | Biographies of Contributors to Report

Michael Chertoff

Michael Chertoff served as Secretary of the U.S. Department of Homeland Security from 2005 to 2009. Before leading the Department of Homeland Security, Mr. Chertoff served as a federal judge on the U.S. Court of Appeals for the Third Circuit. Earlier, during more than a decade as a federal prosecutor, he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism – including the investigation of the 9/11 terrorist attacks.

At The Chertoff Group, Mr. Chertoff provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery. In addition to his role at The Chertoff Group, Mr. Chertoff is also senior of counsel at Covington & Burling LLP, and a member of the firm's White Collar Defense and Investigations practice group.

Mr. Chertoff is a magna cum laude graduate of Harvard College (1975) and Harvard Law School (1978). From 1979-1980 he served as a clerk to Supreme Court Justice William Brennan, Jr.

Paul Schneider

Paul Schneider served as Deputy Secretary for the Department of Homeland Security where he managed day-to-day operations of an organization with approximately 220,000 employees and an annual budget of $52.6 billion. Earlier, as Under Secretary for Management, he was responsible for the department's financial management and for the procurement and

management of such mission-critical assets as information technology systems, facilities and equipment.

At The Chertoff Group, Mr. Schneider counsels clients on budgeting, procurement, and overall management issues related to security programs.

As a defense and aerospace consultant before joining DHS, Mr. Schneider conducted such high-level studies as an analysis for NASA of the risks and benefits of manned space flight. He also served as the Senior Acquisition Executive of the National Security Agency, where he oversaw the development and acquisition of information security programs.

Mr. Schneider holds a degree in nuclear engineering and is a member of the American Society of Naval Engineers, Armed Forces Communications and Electronics Association and the Association of Scientists and Engineers.

Mark Weatherford

Mark Weatherford is a Principal at The Chertoff Group and advises clients on a broad array of cybersecurity services. As one of the nation's leading experts on cybersecurity, Mr. Weatherford works with organizations around the world to effectively manage today's cyber threats by creating comprehensive security strategies that can be incorporated into core business operations and objectives.

Prior to joining The Chertoff Group, Mr. Weatherford served as the U.S. Department of Homeland Security's first Deputy Under Secretary for Cybersecurity within the National Protection and Programs Directorate. In this role, he worked with all national critical infrastructure sectors and federal government agencies to develop an understanding of the cyber threat environment and create more secure IT network operations. Through his leadership, DHS

greatly expanded its efforts to assist private sector organizations in identifying pre-incident vulnerabilities, share actionable cyber threat information, and provide forensics and remediation services. These actions resulted in dramatically improved government-private sector relationships and led DHS to a new level of cybersecurity maturity.

Prior to joining DHS, Mr. Weatherford was Vice President and Chief Security Officer at the North American Electric Reliability Corporation (NERC) where he directed the cybersecurity and critical infrastructure protection program. Prior to NERC, Mr. Weatherford was appointed by Governor Schwarzenegger to serve as California's first Chief Information Security Officer and was also the first Chief Information Security Officer for the State of Colorado, where he was appointed by two successive governors.

Previously, Mr. Weatherford worked at the Raytheon Company where he successfully built and directed the Navy/Marine Corps Intranet Security Operations Center in San Diego, California, and was part of a team conducting security certification and accreditation with the U.S. Missile Defense Agency. As a former U.S. Navy Cryptologic Officer, Mr. Weatherford led the U.S. Navy's Computer Network Defense operations and the Naval Computer Incident Response Team (NAVCIRT).

Mark Weatherford earned a bachelor's degree from the University of Arizona and a master's degree from the Naval Postgraduate School. He also holds a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM) certifications. He was one of the Information Security magazine's "Security 7 Award" winners in 2008, was awarded SC Magazine's prestigious "CSO of the Year" award for 2010, and was named one of the "10 Most Influential People in Government Information Security" by GovInfoSecurity in both 2012 and 2013.

Robert J. Butler

Robert J. Butler is the Chief Security Officer and a Senior Vice President for IO Data Systems LLC ("IO"), a worldwide leader in software-defined modular data center technology, services, and solutions for global financial services firms, other critical infrastructure service companies, and governments. In his current role, Mr. Butler applies federal security standards and commercial best practices to mitigate security issues at IO and its clients, which include owners and operators of systems designated by the U.S. Government as critical infrastructure.

Mr. Butler's distinguished career in information technology, intelligence, and national security spans 35 years in the public and private sectors. Before assuming his present position at IO, he served as the first Deputy Assistant Secretary of Defense for Cyber Policy (August 2009-August 2011.) In that role, Mr. Butler acted as the principal advisor to the Secretary of Defense and other United States Government leaders on the development of cyber strategy and policy, including the creation of federal security standards around critical infrastructure.

He is a retired U.S. Air Force colonel and former member of the Defense Department's senior executive service. In that capacity he served as the Director of Intelligence at the U.S. Transportation Command during Operations Enduring Freedom and Iraqi Freedom; Commander of the Medina Regional Security Operations Center and the National Security Agency's ("NSA's") Texas Cryptologic Center; and Associate Director of the Joint Information Operations Warfare Command. He has also been an Account Executive and senior cyber strategist with Computer Sciences Corporation.

Mr. Butler serves as a Special Government Expert to the Department of Homeland Security, and has also consulted in that capacity for the Office of the Secretary of Defense, the

Air Force Scientific Advisory Board, and other government-sponsored organizations on cybersecurity. He also currently serves as an adjunct fellow at the Center for New American Security and is a senior advisor to The Chertoff Group.

Mr. Butler earned a bachelor's degree of science in computer information systems from Manhattan College and a master's degree in business administration from the School of Business at the University of Maryland. He is a former RAND fellow and has served as a National Defense Fellow at Georgetown University's School of Foreign Service.

Joel F. Brenner

Joel F. Brenner specializes in cyber and physical security, data protection and privacy, intelligence law, the administration of classified information and facilities, and the regulation of sensitive cross-border transactions. He has represented companies and individuals in a wide variety of transactions and proceedings, including sensitive foreign acquisitions involving the Committee on Foreign Investment in the United States, the law governing network operations, the liability of foreign governments, export controls, and internal corporate and government investigations. He has years of experience inside and outside government involving national and homeland security. Mr. Brenner was Senior Counsel at the NSA, advising leadership on the public-private effort to create better security for the Internet. From 2006 until mid-2009, he was the head of U.S. counterintelligence under the Director of National Intelligence and was responsible for integrating the counterintelligence activities of the 17 departments and agencies with intelligence authorities, including the FBI and CIA and elements of the Departments of Defense, Energy, and Homeland Security. From 2002 to 2006, Mr. Brenner was NSA's Inspector General, responsible for that agency's top-secret internal audits and investigations. He

has also served as a prosecutor in the Justice Department's Antitrust Division and has extensive trial and arbitration experience in private practice.

Mr. Brenner holds a J.D. from the Harvard Law School, a Ph.D. from the London School of Economics, and a B.A. from the University of Wisconsin—Madison. He is a member of the American Bar Association's Standing Committee on Law & National Security. He has written about intelligence oversight and presidential authority to suspend or prohibit foreign takeovers of U.S. firms, and he is often quoted in the national media on data security, privacy, and intelligence issues. Mr. Brenner was awarded the Intelligence Community Achievement Medal in July 2009. Mr. Brenner is the author of *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime and Warfare* (Penguin Press, 2011), now available in paperback as *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (Penguin Press, 2013).

Adam Isles

Adam Isles is a Managing Director at The Chertoff Group, where he advises clients on security risk management programs. Mr. Isles has managed security services engagements for clients in a number of industries, including the financial services, retail, and transportation sectors. Mr. Isles also provides market assessment advice for providers of security products, services, and solutions. Prior to joining The Chertoff Group, Mr. Isles worked at Raytheon Company, where he was the Director of Strategy and Policy Consulting for homeland security. In this role, Mr. Isles built and managed a team of subject matter experts responsible for helping homeland security customers analyze mission needs and develop risk management strategies and technology solutions to mitigate security concerns. He is a certified Raytheon Six Sigma specialist.

Previously, Mr. Isles served as the Deputy Chief of Staff at the U.S. Department of Homeland Security, where he worked daily with the Secretary of Homeland Security to coordinate department-wide operations. Before joining the Department of Homeland Security, Mr. Isles served at the U.S. Department of Justice, where he started his legal career as a trial attorney in the Criminal Division in 1997. From 2002 to 2003, he was a Director of International Economic Affairs at the National Security Council. Mr. Isles is currently a Senior Associate (Non-Resident), Homeland Security and Counterterrorism Program at the Center for Strategic and International Studies. He holds a J.D. from Harvard Law School and a B.A. in history from Yale University, and is a member of the New York, Massachusetts, and District of Columbia bars.