NIST Roadmap for Improving Critical Infrastructure Cybersecurity

February 12, 2014

1. Introduction

This companion Roadmap to the *Framework for Improving Critical Infrastructure Cybersecurity* ("the Framework") discusses NIST's next steps with the Framework and identifies key areas of development, alignment, and collaboration. These plans are based on input and feedback received from stakeholders through the Framework development process particularly on the "Areas for Improvement" section of the Preliminary Framework, which has been moved to this document.

2. Evolution of the Cybersecurity Framework

Since Executive Order 13636 was issued, NIST has played a convening role in developing the Framework, drawing heavily on standards, guidelines, and best practices already available to address key cybersecurity needs. NIST also relied on organizations and individuals with experience in reducing cybersecurity risk and managing critical infrastructure.

Moving forward, NIST is committed to help organizations understand and use the Framework. Organizations that are part of the critical infrastructure can use the Framework to better manage and reduce its cybersecurity risks.

Not all critical infrastructure organizations have a mature program and the technical expertise in place to identify, assess, and reduce cybersecurity risk. Many have not had the resources to keep up with the latest cybersecurity advances and challenges as they balance risks to their organizations. NIST intends to conduct a variety of activities to help organizations to use the Framework. For example, industry groups, associations, and non-profits can be key vehicles for strengthening awareness of the Framework. NIST will encourage these organizations to become even more actively engaged in cybersecurity issues, and to promote – and assist in the use of – the Framework as a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks. NIST will build on existing relationships and expand its outreach in these areas, in partnership with the Department of Homeland Security's (DHS) Voluntary Program.

The Framework was intended to be a "living document," stating that it "will continue to be updated and improved as industry provides feedback on implementation. As the Framework is put into practice, lessons learned will be integrated into future versions. This will ensure it is meeting the needs of critical infrastructure owners and operators in a dynamic and challenging environment of new threats, risks, and solutions."

NIST will continue to serve in the capacity of "convener and coordinator" at least through version 2.0 of the Framework. This will ensure that the Framework advances steadily and addresses key areas that need further development.

In the interest of continuous improvement, NIST will receive and consider comments about the Framework informally until it issues a formal notice of revision to version 1.0. At that point, NIST will specify a focus for comments and specific deadlines that will allow it to develop and publish proposed revisions in a timely and transparent fashion.

NIST intends to hold at least one workshop within six months after the Framework's issuance to provide a forum for stakeholders to share experiences in using the Framework. NIST will also hold one or more workshops and focused meetings on specific Areas for Development, Alignment, and Collaboration.

3. Strengthening Private Sector Involvement in Future Governance of the Framework

Even as NIST continues to support and improve the Framework, it will solicit input on options for long-term governance of the Framework including transitioning responsibility for the Framework to a non-government organization. Any transition must minimize or prevent potential disruption for organizations that are using the Framework.

The ideal transition partner (or partners) would have the capacity to work closely and effectively with international organizations, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally. Transitioning to such a partner – along with NIST's continued support - would help to ensure that cybersecurity-related standards and approaches taken by the Framework avoid creating additional burdens on multinational organizations wanting to implement them.

4. Areas for Development, Alignment, and Collaboration

Executive Order 13636 states that the cybersecurity Framework will "identify areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations." Several high-priority areas for development, alignment, and collaboration are listed below based on stakeholder input and are described in the subsections below.

This list of high-priority areas is not intended to be exhaustive. These are important areas identified by stakeholders that should inform future versions of the Framework. They require continued focus; they are important but evolving areas that have yet to be developed or need further research and understanding. While tools, methodologies, and standards exist for some of the areas, they need to become more mature, available, and widely adopted. To be effective in addressing these areas, NIST will work with stakeholders to identify primary challenges, solicit input to address those identified needs, and collaboratively develop and execute action plans for addressing them.

Many of these areas also reflect needed capabilities in the Framework Core. As progress is made in each of these areas, they can be immediately used in conjunction with the Framework to enhance or improve existing cybersecurity

programs. Progress in these areas also becomes candidate improvements to the Framework.

4.1. **Authentication**

Poor authentication mechanisms are a commonly exploited vector of attack by adversaries; the 2013 Data Breach Investigations Report (conducted by Verizon in concert with the U.S. Department of Homeland Security) noted that 76% of 2012 network intrusions exploited weak or stolen credentials. Multi-Factor Authentication (MFA) can assist in closing these attack vectors by requiring individuals to augment passwords ("something you know") with "something you have," such as a token, or "something you are," such as a biometric.

While new authentication solutions continue to emerge, there is only a partial framework of standards to promote security and interoperability. The usability of authentication approaches remains a significant challenge for many control systems, as many existing authentication tools are for standard computing platforms. Moreover, many solutions are geared only toward identification of individuals; there are fewer standards-based approaches for automated device authentication.

The inadequacy of passwords for authentication was a key driver behind the 2011 issuance of the National Strategy for Trusted Identities in Cyberspace (NSTIC), which calls upon the private sector to collaborate on development of an Identity Ecosystem that raises the level of trust associated with the identities of individuals, organizations, networks, services, and devices online. NSTIC is focused on consumer use cases, but the standards and policies that emerge from the privately-led Identity Ecosystem Steering Group (IDESG) established to support the NSTIC – as well as new authentication solutions that emerge from NSTIC pilots – can inform advances in authentication for critical infrastructure as well.

NIST will focus on three areas:

- Continue to support the development of better identity and authentication solutions through NSTIC pilots, as well as an active partnership with the IDESG;
- Support and participate in identity and authentication standards activities, seeking to advance a more complete set of standards to promote security and interoperability; this will include standards development work to address gaps that may emerge from new approaches in the NSTIC pilots.
- Conduct identity and authentication research complemented by the production of NIST Special Publications that support improved authentication practices.

4.2. **Automated Indicator Sharing**

The automated sharing of indicator information can provide organizations with timely, actionable information that they can use to detect and respond to cybersecurity events as they are occurring. Sharing indicators based on information that is discovered prior to and during incident response activities enables other

organizations to deploy measures to detect, mitigate, and possibly prevent attacks as they occur. Organizations tend to share a subset of indicator data to avoid exposing the organization to further risks. This information is shared through various channels including: information sharing communities (e.g., sector-specific ISACs, consortiums), peer-to-peer sharing with selected partners, and exchanges with security service providers. Receiving such indicators allows security automation technologies a better chance to detect past attacks, mitigate and remediate known vulnerabilities, identify compromised systems, and support the detection and mitigation of future attacks.

Organizations use a combination of standard and proprietary mechanisms to exchange indicators that can be used to bolster defenses and to support early detection of future attack attempts. These mechanisms have differing strengths and weaknesses and often require organizations to maintain specific process, personnel, and technical capabilities. Groups of highly capable organizations commonly form communities to share useful indicator data. Established communities tend to grow through addition of newer members with lower capability. To make these communities more effective, appropriate standards need to be defined and then adopted in products to enable organizations of various levels of capability and size to make use of indicators and other related shared information.

NIST will work together with private and public sector organizations to promote a global competitive marketplace of interoperable solutions that enable both small and large organizations to take advantage of indicator sharing. NIST will work with:

- Private sector standards owners, consortia and others in industry-led, consensus-driven international standards organizations to fill current standards gaps based on well-defined use cases and requirements.
- Private and public sector stakeholders to ensure that adequate implementation and common practice guidance is available regarding the generation, use, and sharing of indicator data.

4.3. **Conformity Assessment**

Conformity assessment can be used to show that a product, service, or system meets specified requirements for managing cybersecurity risk. The output of conformity assessment activities could be used to enhance an organization's understanding of its implementation of a Framework profile. Successful conformity assessment provides the needed level of confidence, is efficient, and has a sustainable and scalable business case. Critical infrastructure's evolving implementation of Framework profiles should drive the identification of private sector conformity assessment activities that address the confidence and information needs of stakeholders.

NIST will help ensure that private and public sector conformity assessment needs are met by leveraging existing conformity assessment programs and other activities that produce evidence of conformity. This reduces the resource burden on the private sector. NIST will work with:

- Private sector standards owners, consortia and others who manage conformity assessment programs to help all stakeholders understand how these programs can be further leveraged by those who have the need for conformity demonstration; and
- Private and public sector entities that have a need for conformity demonstration, to help understand how these organizations can leverage existing programs.

4.4. **Cybersecurity Workforce**

A skilled cybersecurity workforce is needed to meet the unique cybersecurity needs of critical infrastructure. There is a well-documented shortage of general cybersecurity experts; however, there is a greater shortage of qualified cybersecurity experts who also have an understanding of the unique challenges posed to particular parts of critical infrastructure. As the cybersecurity threat and technology environment evolves, the cybersecurity workforce must continue to adapt to design, develop, implement, maintain and continuously improve the necessary cybersecurity practices within critical infrastructure environments.

Various efforts, including the National Initiative for Cybersecurity Education (NICE), are currently fostering the training of a cybersecurity workforce for the future, establishing an operational, sustainable and continually improving cybersecurity education program to provide a pipeline of skilled workers for the private sector and government. Organizations must understand their current and future cybersecurity workforce needs, and develop hiring, acquisition, and training resources to raise the level of technical competence of those who build, operate, and defend systems delivering critical infrastructure services.

NIST will continue to promote existing and future cybersecurity workforce development activities (including NICE), including coordinating with other government agencies, such as DHS. NIST and its partners will also continue to increase engagement with academia to expand and fill the cybersecurity workforce pipeline.

Future NIST activities may include:

- Extending and integrating NICE activities across critical infrastructure (CI) sectors to raise cybersecurity awareness;
- Identifying and supporting foundational research opportunities in areas including cybersecurity awareness, training, and education, and security usability;
- Understanding CI cybersecurity workforce needs; and
- Issuing guidelines, tools, and other resources to develop, customize and deliver cybersecurity awareness, training, and education materials.

4.5. **Data Analytics**

Big data and the associated analytic tools coupled with the emergence of cloud, mobile, and social computing offer opportunities to process and analyze structured

and unstructured cybersecurity-relevant data. Issues such as situational awareness of complex networks and large-scale infrastructures can be addressed. The analysis of complex behaviors in these large scale-systems can also address issues of provenance, attribution, and discernment of attack patterns.

Several significant challenges must be overcome for the extraordinary potential of analytics to be realized, including the lack of: taxonomies of big data; mathematical and measurement foundations; analytic tools; measurement of integrity of tools; and correlation and causation. More importantly, the privacy implications in the use of these analytic tools must be addressed for legal and public confidence reasons.

Future NIST activities may include:

- Benchmarking and measurement of some of the fundamental scientific elements of big data (algorithms, machine learning, topology, graph theory, etc.) through means such as research, community evaluations, datasets, and challenge problems;
- Support and participation in big data standards activities such as international standards bodies and production of community reference architectures and roadmaps; and
- Production of NIST Special Publications on the secure application of big data analytic techniques in such areas as access control, continuous monitoring, attack warning and indicators, and security automation.

4.6. **Federal Agency Cybersecurity Alignment**

The Federal Information Security Management Act (FISMA) requires federal agencies to implement agency-wide programs to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA directed NIST to develop a suite of standards and guidelines which, when integrated, provide a Risk Management Framework to help agencies effectively identify, assess, and mitigate risk to agency operations, assets, and individuals.

While developed for federal agency use, these standards and guidelines are frequently voluntarily used by non-federal organizations because of the flexible, risk-based, and cost-effective approach they offer. Specific federal standards and guidelines – often cited by non-Federal participants during development of the Cybersecurity Framework as resources they found useful in managing cybersecurity risk – were included as informative references in the Framework Core.

The Cybersecurity Framework and the NIST Risk Management Framework both seek to achieve the same objective – improved management of cybersecurity risk. It is important that any effort to apply the Cybersecurity Framework across the Federal government complement and enhance rather than duplicate or conflict with existing statute, executive direction, policy, and standards. It should also seek to minimize the burden placed upon implementing departments and agencies by building from existing evaluation and reporting regimes, and encourage common

and comparable evaluation of cybersecurity posture across federal departments and agencies, given diverse requirements and risk environments.

NIST, working with our interagency partners, will:

- Identify areas of alignment between existing Federal Information Processing Standards (FIPS), guidelines, frameworks, and other programs (e.g., Continuous Diagnostics and Mitigation) and the Cybersecurity Framework;
- Identify and prioritize gaps where additional guidance may improve an agency's ability to manage cybersecurity risk, and demonstrate greater alignment with the Cybersecurity Framework; and
- Leverage the Cybersecurity Framework to elevate the use and amplify the effectiveness of new and emerging Federal standards, guidelines, and programs.

4.7. **International Aspects, Impacts, and Alignment**

Globalization and advances in technology have driven unprecedented increases in innovation, competitiveness, and economic growth. Critical infrastructure has become dependent on these enabling technologies for increased efficiency and new capabilities. Many governments are proposing and enacting strategies, policies, laws, and regulations covering information technology for critical infrastructure as a result. Because many organizations and most sectors operate globally or rely on the interconnectedness of the global digital infrastructure, these requirements are affecting, or may affect, how organizations operate, conduct business, and develop new products and services. Diverse or specialized requirements can impede interoperability, result in duplication, harm cybersecurity, and hinder innovation. In turn, this can significantly reduce the availability and use of innovative technologies to critical infrastructures in all industries and hamper the ability of organizations to operate globally and to effectively manage new and evolving risks.

Because the Framework references globally accepted standards, guidelines and practice, organizations domiciled inside and outside of the United States can use the Framework to efficiently operate globally and manage new and evolving risks. Conversely, broad use of the Framework will serve as a model approach to strengthening the critical infrastructure, while discouraging a balkanization caused from unique requirements that hamper interoperability and innovation, and limit the efficient and effective use of resources.

NIST will continue to communicate the intent and approach of the cybersecurity Framework to the international community by:

- Engaging foreign governments and entities directly to explain the Framework and seek alignment of approaches when possible;
- Coordinating with federal agency partners to ensure full awareness with their stakeholder community;
- Working with industry stakeholders to support their international engagement; and

- Exchanging information and working with standards developing organizations, industry, and sectors to ensure the Cybersecurity Framework remains aligned and compatible with existing and developing standards and practices.

4.8. **Supply Chain Risk Management**

Supply chains consist of organizations that design, produce, source, and deliver products and services. All organizations are part of, and dependent upon, product and service supply chains. Supply chain risk is an essential part of the risk landscape that should be included in organizational risk management programs. Although many organizations have robust internal risk management processes, supply chain criticality and dependency analysis, collaboration, information sharing, and trust mechanisms remain a challenge. Organizations can struggle to identify their risks and prioritize their actions—leaving the weakest links susceptible to penetration and disruption. Supply chain risk management, especially product and service integrity, is an emerging discipline characterized by diverse perspectives, disparate bodies of knowledge, and fragmented standards and best practices.

Increasing adoption of supply chain risk management standards, practices and guidelines requires greater awareness and understanding of the risks associated with the time-sensitive interdependencies throughout the supply chain, including in and between critical infrastructure sectors/subsectors. This understanding is vital to enable organizations to assess their risk, prioritize, and allow for timely mitigation.

NIST's activities will focus on engaging stakeholders to:

- Encourage broad industry engagement and leadership in supply chain risk management discussions and activities;
- Promote the mapping of existing supply chain risk management standards, practices and guidelines to the Framework Core;
- Identify challenges in Framework adoption and determine appropriate support to enable effective supply chain risk management; and
- Determine the key challenges to supply chain risk management (e.g. identifying and understanding mission critical functions, their dependencies, and conducting and validating prioritization) to enable more effective Framework implementation.

4.9. **Technical Privacy Standards**

A key challenge for privacy has been the difficulty in reaching consensus on definition and scope management, given its nature of being context-dependent and relatively subjective. The Fair Information Practice Principles (FIPPs), - developed in the early stages of computerization and data aggregation to address the handling of individuals' personal information – have become foundational in the current conception of privacy. They have been used as a basis for a number of laws and regulations, as well as various sets of privacy principles and frameworks around the

world. The FIPPs, however, are a process-oriented set of principles for handling personal information. They do not purport to define privacy in a way that has enabled the development of a risk management model nor do they provide specific technical standards or best practices that can guide organizations in implementing consistent processes to avoid violating the privacy of individuals.

The lack of risk management model, standards, and supporting privacy metrics, makes it difficult to assess the effectiveness of an organization's privacy protection methods. Furthermore, organizational policies are often designed to address business risks that arise out of privacy violations, such as reputation or liability risks, rather than focusing on minimizing the risk of harm at an individual or societal level. Although research is being conducted in the public and private sectors to improve current privacy practices, many gaps remain. In particular, there are few identifiable technical standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties.

To address these gaps and challenges, NIST will first host a privacy workshop in the second quarter of 2014. The workshop will focus on the advancement of privacy engineering as a foundation for the identification of technical standards and best practices that could be developed to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties. Modeled after security engineering, privacy engineering may call for the development of a privacy risk management model, privacy requirements and system design and development. Future NIST activities will build upon the outcomes of the workshop, and NIST will work with private and public sector entities to support improvements in the protection of individuals' privacy and civil liberties while securing critical infrastructure.