White Paper

DHS Response to the NIST Cybersecurity Framework Request for Information

Background:

On February 12, President Obama signed Executive Order 13636: Improving Critical Infrastructure Cybersecurity (EO 13636). EO 13636 is intended to "to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." Central to EO13636 is the development of a Cybersecurity Framework to "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach...to help owners and operators of critical infrastructure identify, assess, and manage cyber risk." On February 26, the National Institute of Standards and Technology (NIST) released a Request for Information (RFI) regarding current risk management practices, the use of existing frameworks, standards, and best practices to manage cybersecurity risk, and industry-specific practices of particular relevance.

The Department of Homeland Security (DHS) is prepared to fully support NIST in the development of the framework and believes its experience in developing the National Infrastructure Protection Plan (NIPP), its role as the government sector lead for multiple infrastructures and the experience it has gained from its emergency response leadership will be a critical source of knowledge that NIST can leverage during the development of the framework. DHS solicited input from its various components and offices, and developed a consolidated set of RFI responses that reflect a broad spectrum of priorities and programs. This White Paper synthesizes the general themes of these consolidated responses, identifies key principles of particular salience to DHS and its mission, and suggests aspects of the Framework that merit emphasis to best reduce or otherwise manage cybersecurity risk to critical infrastructure.

The following DHS components and offices contributed to this response:

- Privacy Office
- Customs and Border Protection (CBP)
- Federal Emergency Management Agency (FEMA)
- National Protection and Programs Directorate (NPPD)/Office of Cybersecurity and Communications (CS&C)
  - National Cybersecurity and Communications Integration Center (NCCIC)
    - United States-Computer Emergency Readiness Team (US-CERT)
    - Industrial Control Systems- Computer Emergency Response Team (ICS-CERT)
  - Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)
  - Federal Network Resilience (FNR)
  - Network Security Division (NSD)
- National Protection and Programs Directorate (NPPD)/Office of Infrastructure Protection (IP)
- United States Secret Service (USSS)
- Science & Technology (S&T)

DHS Response:

Rather than responding to each of the 33 questions in the NIST RFI in turn, this White Paper summarizes DHS input in the context of two associated priorities under EO 13636: the development of a voluntary program to support the adoption of the Cybersecurity Framework and the development of functional performance goals to evaluate progress toward ensuring the provision of essential services under all conditions. Where relevant, this paper also references related DHS mandates under EO 13636 and Presidential Policy Directive-21, including enhanced cybersecurity information sharing, improvements to the

public-private partnership model, development of a national research and development plan, and the revision of the National Infrastructure Protection Plan (NIPP).

Promoting Framework Adoption through the Voluntary Program

EO 13636 mandates that DHS establish "a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure," a requirement that is dependent on the perceived value and costs of the Framework on the part of implementing owners and operators. DHS components and offices offered several recommendations regarding attributes of the Cybersecurity Framework that may encourage broad cross-sector adoption. Notably, DHS respondents suggested that ensuring executive-level understanding of cybersecurity risks and the efficacy of investments in security and resilience is of paramount importance. To this end, adoption of the voluntary Cybersecurity Framework should incentivize proactive investments and measurable improvements, rather than serving as a compliance exercise. The framework must remain a truly voluntary structure, both due to the lack of legal authority to compel participation, but more practically because securing the cyber critical infrastructure is an enormous task in which we all have common interests. The task requires government at all levels, the private sector and individuals to work together cooperatively, something we believe will be more readily achieved in most of the critical infrastructure sectors and sub-sectors using positive incentives than with regulatory disincentives. DHS is chairing a working group to identify potential incentives to promote Framework adoption; however, the subjective effectiveness of the Framework in reducing cybersecurity risk may provide an additional incentive toward adoption.

Importantly, the diversity in risk profiles between sectors may result in a scenario in which specific actions to improve security and resilience may be highly impactful in a particular sector while relatively inconsequential in another. Therefore, the Cybersecurity Framework should provide sufficient flexibility to tailor specific actions to best reduce organizational and functional risk. Of note, the DHS Cyber Assessment Risk Management Approach (CARMA) provides a methodology for sector stakeholders to define key business functions that must be protected, and identifies risks posed to their functional viability. Both CARMA and the Cybersecurity Framework will rely on input from relevant subject-matter experts and sector best practices to identify the extent and implications of cybersecurity risk and the effective mitigations thereof. To this end, the Cybersecurity Framework may look to the Information Technology and Emergency Services Sector CARMA assessments for an example of risk-based analyses that can effectively inform stakeholder decisions.

The identification of critical infrastructure where a cybersecurity incident could "reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security" will support the Cybersecurity Framework in reducing national-level cybersecurity risk.. DHS plans to leverage the Cybersecurity Framework to guide its legacy programs to assess, on a voluntary basis, cyber and physical risk across critical infrastructure and systems. Further, as referenced above, the CARMA methodology allows the identification and evaluation of *nth*-order impacts and associated cascading effects, enabling the recognition of dependent and interdependent infrastructure that should adopt the voluntary Cybersecurity Framework. A similar approach could build upon the initial list of Cyber-Dependent Infrastructure to identify and understand non-obvious infrastructure relationships, including dependence upon shared information and communications technology, which could result in cascading impacts of national or regional significance.

DHS components and offices noted a number of existing standards and best practices that could be incorporated in the Cybersecurity Framework. The inclusion of these standards and best practices will both promote the validity of the framework and incentivize adoption by minimizing the implementation burden on organizations already compliant with referenced standards. DHS will continue to work with NIST, other government agencies, and industry to research and define process (e.g., NIST publications), technical (e.g., RFC2827), and privacy/civil rights/civil liberties (e.g., Consumer Privacy Bill of Rights) standards that support the Cybersecurity Framework.

DHS applauds NIST for taking steps to ensure that privacy and civil liberties protections will be built into the Cybersecurity Framework. With respect to privacy in particular, DHS suggests that a core set of resources[1] be drawn upon to build the privacy controls within the Framework. Although some of the resources apply to the government and others to the private sector, they are all based upon the Fair Information Practice Principles (FIPPs), which are well accepted both across the federal government and the private sector. NIST should consider these resources in light of the specific context in which owners and operators of critical infrastructure and other interested entities operate when building the privacy controls into the Cybersecurity Framework. DHS acknowledges also that care must be taken as it and the Sector Specific Agencies implement the framework to ensure that the implementation is in fact voluntary, except in those limited, regulated subsectors of the critical infrastructure where risk-based analysis dictates a stronger government response is needed, and where legal authority authorizes such steps.

While voluntary consensus standards are a critical component of the cybersecurity landscape, DHS also recognizes the rapid evolution of technology and the demonstrated ability of malicious actors to leverage technology to achieve their goals. As such, any successful framework must allow for rapid innovation and technology adaptation by all stakeholders, including the owners and operators of critical infrastructure. The Cybersecurity Framework, itself, should also be agile such that it can adapt to changing risk environments over time. Balancing the need for mission-focused technological agility with long-term stability via standards should be a priority of the framework.

Ensuring Framework Effectiveness with Functional Performance Goals

DHS is required under EO 13636 to develop performance goals that are based upon the essential functions provided by the 16 critical infrastructure sectors. These performance goals will establish national-level guidance to achieve desired outcomes for infrastructure security and resilience (through the provision of critical services to supported populations and dependent infrastructure). However, their usefulness will increase as they are tailored and adapted for use by individual owners and operators of critical infrastructure. Adopters of the performance goals would establish their own associated measures and targets related to the desired outcomes. DHS components and offices noted the need to understand the sector- and infrastructure-specific essential functions that could be rendered vulnerable by a cybersecurity incident, and how the Cybersecurity Framework can best assure the availability of such functions across sectors. The use of functional performance goals may also assist infrastructure owners and operators in implementing the Cybersecurity Framework across multiple constituent organizations, including across mission and business functions, shared information systems, and partially-held or subsidiary organizations.

Constraints, such as competing legal and regulatory requirements (including at the state, federal, and international levels) and budgetary limitations, may affect the extent of Framework implementation. . The use of performance goals will be an effective tool to ensure that critical infrastructure owners and operators invest in risk management measures that are driven by functional requirements while remaining aware of cost constraints.. The Framework and associated performance goals will further support the mandate, under Presidential Policy Directive 21, for DHS to update the NIPP by "identifying a risk management framework to be used to strengthen the security and resilience of critical infrastructure; the methods to be used to

[1] These resources include:

- Consumer Privacy Bill of Rights: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf
- NSTIC Principles: http://www.nist.gov/nstic/privacy.html
- Final Public Draft, NIST Special Publication 800-53, " Security and Privacy Controls for Federal Information Systems and Organizations," Revision 4: http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf
- DHS's FIPPs in DHS Directive 047-0, "Privacy Policy and Compliance" http://www.dhs.gov/xlibrary/assets/foia/privacy-policy-compliance-directive-047-01.pdf

prioritize critical infrastructure; the protocols to be used to synchronize communication and actions within the Federal Government; and a metrics and analysis process to be used to measure the Nation's ability to manage and reduce risks to critical infrastructure." In this context, the Cybersecurity Framework may be considered a baseline for cybersecurity risk management. Furthermore, the performance goals can be tailored to sectors and sub-sectors for use in sector-specific planning and reporting.

Conclusion

The Department of Homeland Security is committed to working with critical infrastructure owners and operators, NIST, and other Federal, State, local and private sector stakeholders to develop a Cybersecurity Framework that supports research, rapid innovation and technology adaptation while balancing the need for long-term, standards-based stability. The framework should provide each of its adopters, whether critical infrastructure or otherwise, a clear and accessible approach to cybersecurity risk reduction and management that can be tailored to specific business models while accommodating standards and best practices that many adopters already use. The performance goals will enable adopters to link cybersecurity initiatives to business mission activities. They will provide a business-focused, outcome-oriented construct through which to communicate the importance of cybersecurity investments and activities, including those undertaken pursuant to the adoption of the Cybersecurity Framework.