INSA

INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Thursday, October 9, 2014

Dear Ms. Honeycutt:

Forwarded herewith is INSA's response to NIST's Request for Information on "Experience With the Framework for Improving Critical Infrastructure Cybersecurity." We appreciate the opportunity to provide input from our members on this critically important initiative to our national security. Your consideration is greatly appreciated.

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions. As a nonprofit, nonpartisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities. INSA has more than 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

Should you have any questions or would like additional information, please contact Ryan Pretzer at rpretzer@insaonline.org or (703) 224-4672.

Respectfully,

Joseph R DeTrani

Ambassador Joseph R. DeTrani
President
Intelligence and National Security Alliance

INSA INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Comments on *Experience with the Framework for Improving Critical Infrastructure Cybersecurity*

Response to NIST RFI Prepared by the Intelligence and National Security Alliance's Cyber Intelligence Task Force

Introduction

The Intelligence and National Security Alliance (INSA), as a nonpartisan, nonprofit organization that brings members of the government, private sector and academia together to address national security challenges, welcomes the opportunity to comment on the Framework and share the collective insight of its Cyber Intelligence Task Force members ("the Task Force").

Specifically, the Task Force seeks to provide comment on the question, "Are key cybersecurity issues and opportunities missing that should be considered as priorities, and if so, what are they and why do they merit special attention?" and put forth *cyber intelligence* as a discipline that should be more explicitly represented and explained within the Framework and Roadmap.

The following comments illustrate how a cyber intelligence function would complement the existing framework and help organizations develop a more comprehensive and proactive cybersecurity posture. Recommendations for specific references to the principles and practices of cyber intelligence in the Framework also are included for consideration.

The Case for Cyber Intelligence

The feedback the Task Force has received in conversations with government and private sector actors in critical infrastructure suggests that security operations personnel are frustrated in their ability to implement the framework because they are:

a) overwhelmed with a barrage of relevant and irrelevant threat-related data from multiple feeds;
b) unable to translate that data into meaningful, actionable insights; and
c) find it difficult to communicate the implications of threats and risk for decisions makers at all levels of the enterprise.

From our perspective, many of these challenges arise from the relative absence of a cyber intelligence discipline or function in the cyber domain. *Cyber intelligence*, as we conceive of it, comprises both the process and the product of collecting, analyzing and disseminating actionable information concerning the capabilities, intentions, motivations and activities of potential adversaries and competitors in the cyber domain.

If the cyber intelligence function were more explicitly represented and explained within the existing Framework, adopting organizations could:

a) organize threat feeds and prioritize data through the development of a collection management plan;
b) translate data into meaningful, actionable insights by applying analytic methodologies; and
c) contextualize and communicate the implications of threats and risk to decisions makers at all levels of the enterprise.

The Task Force believes that effective cyber intelligence can guide cybersecurity planning and operations. An intelligence-driven approach to cybersecurity:

- assists cybersecurity professionals in identifying high-risk areas, discerning threat origins and understanding malicious actors' intentions and motivations, providing a wide understanding of the environment;
- helps security operators translate a wide range of data points and sources into actionable information;
- transforms an organization's cybersecurity posture from reactive to proactive;
- helps organizations evolve from static, perimeter-oriented network defenses toward more dynamic and adaptive approaches to countering complex and evolving threats; and
- enables a continuous assessment of the threat environment, its implications for an organization's enterprise security activity, and the potential impacts on business and mission capabilities.

The Framework seeks to guide organizations' cybersecurity activities as part of their broader risk management plans. We agree that risk management is the appropriate frame for organizations to effectively mitigate and respond to cyber threats. To do so effectively, however, organizations must be empowered to understand and adapt to an evolving threat.

Cyber threats do not occur in a vacuum; rather, they are often the result of actions by threat actors whose intent, capability, and desired outcomes inform their malicious activities, as well as the organizations they target and impact. These dynamic threats demand that organizations implement a threat-aware risk management program. The Framework would be supported by a mechanism to help organizations integrate threat awareness within risk management processes. We believe that cyber intelligence is that mechanism.

Cyber intelligence enables organizations to inform their risk management processes with a strong understanding of cyber threats, and to make informed assessments about the likelihood and impact that a specific cyber threat category poses to the organization. This intelligence-led, threat-aware approach is consistent with NIST Special Publication 800-30, *Guide for Conducting Risk Assessments*, in which Chapter 2.3.1 on Risk Models states:

> *Understanding adversary-based threat events gives organizations insights into the capabilities associated with certain threat sources. In addition, having greater knowledge about who is carrying out the attacks gives organizations a better understanding of what adversaries desire to gain by the attacks.*

In a sense, we propose that NIST 800-30 be extended into the Framework through the concept of cyber intelligence. We offer the following language, at the appropriate bullet points below, to illustrate how the principles and practices of cyber intelligence may be better represented within the Framework and Roadmap.

Recommendations

2.1 Framework Core

ID – Identify

- *Asset Management*
- *Business Environment* – In Framework implementation, this category of activity should explicitly include an assessment and understanding of the character of the threats; the motivations, intentions and targets of potential actors; and the broader strategic/operating environment.
- *Governance*
- *Risk Assessment* – Risk Assessment is an important part of intelligence-driven cybersecurity, but the function of Risk Assessment does not subsume cyber intelligence. In Framework implementation, this category of activity should explicitly include as part of threat characterization (and information about threats) not just technical data, but characteristics of, origin, actors, intentions, capabilities, and activities. The adversary-based threats considerations presented in NIST 800-30, *Guide for Conducting Risk Assessments,* provide a strong model for how threat characterization informs organizations' assessments of the likelihood, impact and risk of specific threat scenarios. Intelligence-driven processes, meanwhile, enable organizations to assess which threat scenarios and adversaries are most relevant to their operations.
- *Risk Management Strategy* – In Framework implementation, this category of activity should explicitly include enterprise-wide risk profiles and priorities. It should address how information gathered from industry and government sources is used to create actionable intelligence data, which helps the organization to align its asset priorities with organization-specific threats, risks and hazards.

PR – Protect

- *Access Control*
- *Awareness and Training*
- *Data Security*
- *Information Protection Processes and Procedures* – In Framework implementation, this category of activity should explicitly include how operational data (intelligence) is captured, managed, used and protected across the enterprise. And it should also explicitly include counterintelligence practices for protecting the supply chain and mitigating insider threat.
- *Maintenance*
- *Protective Technology*

DE – Detect

- *Anomalies and Events* – In Framework implementation, this category of activity should explicitly include *interpretation* and *contextualization* of anomalies. Behavioral and actor information should be routinely included in "event data" to better understand threat actors' motivations, intentions, and capabilities. Doing this creates the intelligence that is necessary to manage and enhance the enterprise security posture.
- *Security Continuous Monitoring* - In Framework implementation, this category of activity explicitly includes how analyses of data gathered during Continuous Monitoring can lead to critical and actionable insights. Monitoring over time also illuminates patterns of behavior and activity that permit security operators to better discern a threat actor's intent, and to prepare and respond accordingly.
- *Detection Processes* – In Framework implementation, this category of activity should include nontechnical activity and trends – e.g., geopolitical, social, industry, economic and motivational aspects of threat actors. This information should be collected from a variety of sources to facilitate a more holistic view of the threats and how to manage them. In addition, the Framework should advocate for organizations to seek detection information and indicators of compromise that are specifically relevant to their industry, sector or vertical.

RS – Response

- *Response Planning* – In Framework implementation, this category of activity should explicitly include both technical and nontechnical response options. Courses of action for response planning are best informed by comprehensive, actionable intelligence.
- *Communications*
- *Analysis* – When organizations detect threat activity, it should be evaluated in light of what industry peers have experienced and the probable intents and motivations of threat actors involved in the threat activity. These processes will enable

organizations to perform threat-informed impact assessments and appropriately communicate the implications of threat activity to stakeholders in the business.

- *Mitigation*
- *Improvements*

RC – Recover

- *Recovery Planning*
- *Improvements*
- *Communications*

2.2 Framework Implementation Tiers

- Tiers characterize an organization's practices and reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.
- **Tier 1: Partial – informal, unsystematic, unaware, case by case, isolated**
    a. Threats and information about threats are seen not just as technical but include actors, intentions, capabilities, and activities.
- **Tier 2: Risk Informed – approved, prioritized, aware, internal info sharing, not connected**
    a. Threats and information about threats are seen not just as technical but include actors, intentions, capabilities, and activities.
    b. Operating environments include attack surface and strategic/operating environment for attackers and business.
    c. The organization analyzes and disseminates information about the vulnerability of valued assets in relation to the risk posed by actual and potential threats.
- **Tier 3: Repeatable - formalized, consistent, updated, receives external info**
    a. Threats and information about threats are seen not just as technical but include actors, intentions, capabilities, and activities.
    b. Operating environments include attack surface and strategic/operating environment for attackers and business.
    c. The organization analyzes and disseminates information about the vulnerability of valued assets in relation to the risk posed by actual and potential threats.
    d. The organization ingests intelligence from industry peers and external partners about current threat activity impacting the organization's vertical, as well as changes to the TTPs of threat actors that may target the organization.
- **Tier 4: Adaptive - dynamic, adaptive, integrated, learning, reciprocal use of information**
    a. Threats and information about threats are seen not just as technical but include actors, intentions, capabilities, and activities.
    b. Operating environments include attack surface and strategic/operating environment for attackers and business to include nontechnical activity and trends – e.g., geopolitical, social, industry, economic.

c. The organization analyzes and disseminates information about the vulnerability of valued assets in relation to the risk posed by actual and potential threats.
d. The organization ingests intelligence from industry peers and external partners about current threat activity impacting the organization's vertical, as well as changes to the TTPs of threat actors that may target the organization.
e. Security policies include counterintelligence practices for protecting assets of value, the supply chain and mitigating insider threat.
f. The organization continuously collects, processes, analyzes, and disseminates information about the vulnerability of valued assets in relation to the risk posed by the evolving array of internal and external threats, and uses that information to guide its efforts to Identify, Protect, Detect, Respond, and Recover at the strategic, operational, and tactical levels.

2.3 Framework Profile

- Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.
- Profile and alignment should include assessments of potential adversaries, competitors and threat actors; their capabilities, intentions and activities; and the "attack surface" or context in which they operate. This includes an internal review of the organization's strengths and weaknesses relative to its risk tolerance and security posture.

Conclusion

The INSA Cyber Intelligence Task Force appreciates the opportunity to provide this feedback on the value of cyber intelligence and its role in helping organizations develop a more comprehensive and proactive cybersecurity posture. We look forward to continued dialogue on the important work NIST and its many partners have undertaken to design the Framework.