National Institute of Standards and Technology

Framework for Improving Critical Infrastructure Cybersecurity

Draft Version 1.1

Request for Comment

April 17, 2017

Ernst & Young LLP
220 South Sixth Street, Suite 1400
Minneapolis, MN 55402

Tel: +1 612 371 6344
Fax: +1 612 339 1726
www.ey.com

Edwin Games
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

April 17, 2017

Dear Mr. Games,

Ernst & Young LLP (EY) is delighted to have the opportunity to respond to your request for comment (RFC) supporting the *Framework for Improving Critical Infrastructure Cybersecurity,* Draft Version 1.1, 10 January 2017. Our comments are based on extensive experience implementing the Framework internally, in addition to helping our public and private clients manage risk by engaging the appropriate people, processes, and technology capabilities.

Cybersecurity risk management demands adaptable, scalable and practical approaches to the prevention, detection, delay and remediation of breaches faced by enterprises of all sizes. EY commends the National Institute of Standards and Technology (NIST) on its continued work on the Framework, which represents a significant step toward broadly applicable cybersecurity guidance for critical infrastructure organizations and others that seek to improve their cybersecurity policies and procedures. The Framework's structure and content, particularly the reliance on well-known cybersecurity guidelines, present a baseline for organizations to develop and assess cybersecurity risk management as needed for their business objectives.

EY applauds NIST's grassroots effort to develop and revise the Framework by hosting workshops and meeting with stakeholders to solicit feedback. Posting Framework drafts and stakeholder comments for public review also exemplifies NIST's transparent process.

Sincerely,

Ernst & Young LLP

Overview

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders.

EY is a leading provider of cybersecurity advisory services and has been recognized by numerous industry analysts for its work in this area. Our Cybersecurity practice helps clients identify and address the cyber risks that impact their business strategies and growth agendas. We leverage industry-leading standards, including the Framework, in our service delivery.

EY's purpose is to build a better working world, and our interest in supporting revisions to the Framework stems from this purpose. We recognize that strong, foundational standards that are able to adapt to changes in technology, threats and markets help organizations improve risk management and breach response. The Framework is a living document that was designed to adapt to an ever-changing cybersecurity environment.

EY's comments are focused on the following Framework topics:

1. **Methodology to Protect Privacy and Civil Liberties (Section 3.6).** EY recommends strengthening this section by providing a greater focus on the confidentiality of assets containing personally identifiable information (PII).
2. **Identity Management and Access Control (PR.AC).** EY recommends refining this category's language to improve authentication, authorization and identity proofing.
3. **Measuring and Demonstrating Cybersecurity (Section 4.0).** EY suggests a tighter relationship between the Framework and NIST Special Publication (SP) 800-53 (R4): Security and Privacy Controls for Federal Information Systems and Organizations, 1 April 2013. EY also recommends that additional NIST publications should be referenced, including SP 800-82 (R2), Guide to Industrial Control Systems (ICS) Security, 1 February 2015, and SP 800-37 (R1), Guide for Applying the Risk Management Framework to Federal Information Systems, 1 February 2010.
4. **Cyber Threat Intelligence (ID.RA-2).** EY agrees with NIST's decision to expand the definition of the Core's Risk Assessment category to include Cyber Threat Intelligence (CTI). EY also feels that an additional appendix would be appropriate to examine CTI's relation to risk, specifically examining CTI subscriptions and intelligence platforms, programs and assessments, and operationalizing CTI.
5. **Cyber Supply Chain Risk Management (ID.SC).** EY suggests clarifying inconsistencies between Framework Draft Version 1.1 (01/10/2017) and previous NIST guidance, including SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, 1 April 2015.

1. Methodology to protect privacy and civil liberties

Privacy is a basic human right, as interpreted by the US Supreme Court through a variety of opinions over the years. Safeguarding privacy and other civil liberties is foundational to the ethical operation of government services and infrastructure, and critical to sustaining public trust.

Privacy laws of the United States deal with several different legal concepts. One is the invasion of privacy, a tort based in common law allowing an aggrieved party to bring a lawsuit against an individual who unlawfully intrudes into his or her private affairs, discloses his or her private information, publicizes him or her in a false light, or appropriates his or her name for personal gain.

The essence of the law derives from a right to privacy, defined broadly as "the right to be left alone." It usually excludes personal matters or activities that may reasonably be of public interest, like those of celebrities or participants in newsworthy events. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating the right. These privacies include the Fourth Amendment right to be free of unwarranted search or seizure, the First Amendment right to free assembly, and the Fourteenth Amendment due process right, recognized by the Supreme Court as protecting a general right to privacy within the family.

The development of robust cybersecurity capabilities can sometimes come at the cost of civil liberties. For example, excessive monitoring of employee and customer behavior pushes the boundaries and interpretation of privacy rights. In its current draft, the Framework offers constructive and useful considerations that can serve as a counterweight to overzealous security efforts. The considerations — divided into governance, access management, training, activity monitoring and response activities — are high-level, generally calling for appropriate policies, privacy risk reviews, and training and awareness activities. Below we recommend the inclusion of certain other considerations. We also recommend that the considerations be integrated into other areas of the Framework to better guide consistent implementation.

EY recommends adding the following blue text to incorporate privacy safeguards in a holistic manner.

Page #	Current	Proposed updates
3	Recognizing the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities.	Recognizing the value of privacy and the role that the protection of privacy and civil liberties plays in creating greater public trust, the Executive Order requires that the Framework include a methodology to protect individual privacy and civil liberties when critical infrastructure organizations conduct cybersecurity activities.
14	A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as summarized in a Framework Profile.	A key milestone of the design phase is validation that the system cybersecurity specifications match the needs and risk disposition of the organization as summarized in a Framework Profile. The design phase should also incorporate privacy risk reviews and other safeguards to help prevent specifications from having an undue impact on civil liberties.

Page #	Current	Proposed updates
16	Next, it creates a prioritized action plan to address those gaps – drawing upon mission drivers, a cost/benefit analysis, and risk understanding – to achieve the outcomes in the Target Profile.	Next, it creates a prioritized action plan to address those gaps – drawing upon mission drivers, a cost/benefit analysis, potential impacts to civil liberties, and risk understanding – to achieve the outcomes in the Target Profile.
19	Governance of cybersecurity risk ▶ An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program	Bullet point should be rewritten for clarity and consistency: Process is in place to identify cybersecurity and privacy risks and develop mitigating approaches to such risks. Risk responses should consider the privacy implications of the cybersecurity program.
19	Governance of cybersecurity risk ▶ Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements	Bullet point should be appended: ▶ Process is in place to support compliance of cybersecurity activities with applicable privacy laws, regulations, and Constitutional requirements. The process should include a mechanism to monitor privacy laws and regulations governing the collection and processing of personal information.
19	Approaches to identifying and authorizing individuals to access organizational assets and systems. ▶ Steps are taken to identify and address privacy implications of access control measures to the extent that they involve collection, disclosure, or use of personal information	Bullet point should be rewritten for clarity: ▶ Logical access and administrative controls are in place to protect personal information from unauthorized access or disclosures.
20	Governance of cybersecurity risk ▶ An organization's assessment of cybersecurity risk and potential risk responses considers the privacy implications of its cybersecurity program ▶ Individuals with cybersecurity-related privacy responsibilities report to appropriate management and are appropriately trained	Add bullet point: ▶ New or updated technologies, systems and processes that collect and/or process personal information should be assessed for their privacy impact on personal information.

Page #	Current	Proposed updates
20	Awareness and training measures ▶ Applicable information from organizational privacy policies is included in cybersecurity workforce training and awareness activities ▶ Service providers that provide cybersecurity-related services for the organization are informed about the organization's applicable privacy policies	Bullet point should be rewritten for clarity: ▶ Service providers that provide cybersecurity-related services for the organization, at minimum, should be informed about the organization's applicable privacy policies. Add bullet points: ▶ Process is in place to monitor employee compliance with privacy requirements. ▶ Process is in place to monitor service provider adherence to privacy requirements.
20	Anomalous activity detection and system and asset monitoring ▶ Process is in place to conduct a privacy review of an organization's anomalous activity detection and cybersecurity monitoring	Add bullet point: ▶ Process is in place to identify, manage and resolve privacy and security incidents.
20	Response activities, including information sharing or other mitigation efforts	Add bullet points: ▶ Personal information should not be retained for longer than necessary for business purposes. ▶ Personal information should be securely deleted once it has reached its retention period or is no longer necessary.

Page #	Current	Proposed updates
28, 29	Does not include guidance for contents of "privacy reviews" suggested throughout bullet points on pages 28 and 29.	Add: Privacy Review Considerations When conducting privacy reviews in the above circumstances, the following should be considered, as relevant: ▶ Personal information is not collected unless there is a legitimate business purpose for doing so. ▶ Personal information is not retained past the point for which there is a legitimate business purpose. ▶ Access to personal information is not granted to individuals, groups or third parties who do not have a legitimate business reason for access. ▶ Customers and personnel are notified of privacy safeguards in place. ▶ Personal information is kept accurate.
33	Awareness and Training (PR.AT-3) Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities.	Add: The process should include the following requirements: assess privacy and security controls at third-party vendors that will be provided access to personal information; include privacy requirements in contractual agreements for the protection of shared information; and obtain ongoing assurances that the third party is protecting personal information, as agreed to in the contract, as appropriate with regard to the nature of the personal information in question.

EY believes these updates will help Framework users implement cybersecurity controls to improve the cybersecurity posture of their respective organizations, while limiting the impact to privacy and other civil liberties.

2. Identity management and access control

Effective and robust identity management and access control is fundamental to achieving and sustaining compliance, operational efficiency and cost containment. Additionally, a structured and methodical approach with strong governance while implementing these controls will help sustain improved security and risk reduction across the enterprise.

EY recommends the following updates highlighted in blue text:

Page #	Current	Proposed updates
ii	Update: Refinements to better account for authentication, authorization, and identity proofing. Description of Update: The language of the Access Control Category has been refined to account for authentication, authorization, and identity proofing. A Subcategory has been added to that Category. Finally, the Category has been renamed to Identity Management and Access Control (PR.AC) to better represent the scope of the Category and corresponding Subcategories.	Update: Refinements to better account for authentication, authorization, identity proofing and access management. Description of Update: The language of the Access Control Category has been refined to account for authentication, authorization, identity proofing and access management. A Subcategory has been added to that Category. Finally, the Category has been renamed to Identity Management and Access Control (PR.IA) to better represent the scope of the Category and corresponding Subcategories.
8	Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."	Categories are subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management" and "Detection Processes."
26	Function: Detect Category Unique Identifier: Does not include "IA"	Function: Detect Category Unique Identifier: DE.IA
26	Function: Detect Category: Does not include "Identity Management and Access Control"	Function: Detect Category: Identity Management and Access Control
32	PR.AC-2: Physical access to assets is managed and protected	PR.IA-2: Physical access to authorized assets is provisioned, managed, de-provisioned and validated according to the level of risk the access poses.
32	PR.AC-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate	PR.IA-6: Identities are proofed and bound to credentials, and asserted in interactions when appropriate. A standard unique identifier is associated with users requiring access to authorized assets. Users are authenticated according to the level of risk their access poses.

Page #	Current	Proposed updates
42	Does not include DE.IA-1	DE.IA-1: Access certification of users is performed according to the level of risk their access poses to help guarantee that user access remains appropriate for their job function.

EY believes these access control and identity management updates will help Framework users implement cybersecurity controls and achieve results outlined in the subcategory section, thereby improving the cyber posture of the organization.

3. Measuring and demonstrating cybersecurity

EY proposes incorporating more quantifiable measurements, or Key Performance Indicators (KPIs), into the Framework to gauge whether cyber objectives are achieved. The cybersecurity outcomes of the Core are the basis for a comprehensive set of cybersecurity management metrics. The aggregate of these metrics affects cybersecurity risk.

Page #	Current	Proposed updates
21	"The ability of an organization to determine cause-and-effect relationships between cybersecurity and business outcomes is dependent on the accuracy and precision of the measurement systems…"	Recommend deleting this paragraph. This is generally not true. Measurement systems are useful to track control effectiveness, but business outcomes are better analyzed with cost controls weighed against risk factors, such as business-specific threats, vulnerabilities and impacts.
21	"To mitigate undue cost to the organization, the accuracy and expense of a system need only match the required measurement accuracy of the corresponding business objective."	Recommend this sentence be clarified. It is unclear how an organization would measure the accuracy of most business objectives.
21	4.1. Correlation to Business Results	Recommend removing section 4.1. This section generally discusses the complexities involved with linking cybersecurity outcomes with business objectives. Links between business objectives and cybersecurity are important, but probably cannot be adequately addressed here. Further, the issues described in this section tend to veer away from the Core.
31	ID.SC-3. Suppliers and partners are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Cyber Supply Chain Risk Management Plan.	Recommend adding informative reference to NIST SP 800-53 (R4): SA-4: Acquisition Process

In addition to the proposed editorial comments noted above, we recommend that NIST consider the following conceptual feedback to enhance the effectiveness of this section:

- SP 800-55 (R1), Performance Measurement Guide for Information Security, 1 July 2008, should be incorporated into the Framework Draft. SP 800-55 (R1) assists in the development, selection and implementation of measures to be used at the information system and program levels. These measures indicate the effectiveness of security controls applied to information systems and supporting information security programs. These measures facilitate decision-making, improve performance and increase accountability through the collection, analysis and reporting of relevant performance-related data. This linkage will also provide a method to tie the implementation, efficiency and effectiveness of information system and program security controls to an organization's success in achieving its mission.

SP 800-55 (R1) provides a quantitative approach to measuring and analyzing security control implementation and effectiveness at the information system and program levels, aggregated across multiple individual efforts. It also provides an approach for aggregating information from multiple information systems to measure and analyze information security from an enterprise-level perspective.

- A mature program normally uses multiple tracking mechanisms to document and quantify various aspects of its performance. As more data becomes available, the difficulty of measurement decreases and the ability to automate data collection increases.

As an example, the following table measures Access Control (AC) at the system level:

Measure 3: Access Control (AC) (system level)

Field	Data
Measure ID	Remote Access Control Measure 1 (or a unique identifier to be filled out by the organization)
Goal	▶ *Strategic goal:* make certain an environment of comprehensive security and accountability for personnel, facilities and products ▶ *Information security goal:* Restrict information, system and component access to individuals or machines that are identifiable, known, credible and authorized
Measure	Percentage (%) of remote access points used to gain unauthorized access ▶ NIST SP 800-53 Controls: AC-17; Remote Access
Measure type	Effectiveness/efficiency
Formula	(Number of remote access points used to gain unauthorized access/total number of remote access points) *100
Target	This should be a low percentage defined by the organization.

Field	Data
Implementation evidence	1. Does the organization use automated tools to maintain an up-to-date network diagram that identifies all remote access points (CM-2)? ___ Yes ___ No 2. How many remote access points exist in the organization's network? _____ 3. Does the organization employ Intrusion Detection Systems (IDS) to monitor traffic traversing remote access points (SI-4)? ___ Yes ___ No 4. Does the organization collect and review audit logs associated with all remote access points (AU-6)? ___ Yes ___ No 5. Does the organization maintain a security incident database that identifies standardized incident categories for each incident (IR-5)? ___ Yes ___ No 6. Based on reviews of the incident database, IDS logs and alerts, and/or appropriate remote access point log files, how many access points have been used to gain unauthorized access within the reporting period? _____
Frequency	Collection frequency: organization-defined (example: monthly) Reporting frequency: organization-defined (example: quarterly)
Responsible parties	▶ Information owner: Computer Security Incident Response Team (CSIRT) ▶ Information collector: System Administrator or Information System Security Officer (ISSO) ▶ Information customer: Chief Information Officer (CIO), Senior Agency Information ▶ Security Officer (SAISO) (e.g., Chief Information Security Officer [CISO])
Data source	Incident database, audit logs, network diagrams, IDS logs and alerts
Reporting format	Stacked bar chart, by month, that illustrates the percentage of remote access points used for unauthorized access vs. the total number of remote access points

Source: SP 800-55 (R1), page A-4

EY recommends that the following cyber measures, outlined in SP 800-55 (R1), be incorporated into the Framework Draft to provide more quantifiable measurements to determine cyber efficacy:

Measure #	Measure name	Level
1	Security Budget	Program level
2	Vulnerability Management (VM)	Program level
3	Access Control (AC)	System level
4	Awareness and Training (AT)	Program level
5	Audit and Accountability (AU)	System level
6	Certification, Accreditation, and Security Assessments (CA)	Program level
7	Configuration Management (CM)	Program level
8	Contingency Planning (CP)	Program level
9	Identification and Authentication (IA)	System level
10	Incident Response (IR)	Program level and system level
11	Maintenance (MA)	System level
12	Media Protection (MP)	Program level and system level
13	Physical and Environmental (PE)	Program level
14	Planning (PL)	Program level and system level
15	Personnel Security (PS)	Program level and system level
16	Risk Assessment (RA)	System level
17	System and Services Acquisition (SA)	Program level and system level
18	System and Communications Protection (SC)	Program level
19	System and Information Integrity (SI)	Program level and system level

4. Cyber threat intelligence

EY agrees with NIST's decision to expand the definition of the Core's Risk Assessment category to include ID.RA-2 Cyber Threat Intelligence. EY also believes that an additional appendix would be appropriate to examine CTI's importance in threat-informed risk management. This needs to be better tied to vulnerability management and attack surface reduction. The appendix would help explain how the entire threat landscape intersects with vulnerabilities and the attack surface.

What is Cyber Threat Intelligence?

Cyber Threat Intelligence (CTI) is an advanced process that enables an organization to gather valuable insights based on the analysis of contextual and situational threats and associated risks. It can be tailored to an organization's specific threat landscape, its industry and markets.

The process manages the collection, analysis, integration and production of previously disjointed information for the purpose of extracting holistic, evidence-based insights regarding an organization's unique threat landscape. This intelligence can make a significant difference to an organization's ability to anticipate and respond to breaches before and after they occur.

Leveraging CTI

Today's market emphasis is on delivering CTI in the form of subscriptions and intelligence visualization platforms; however, because subscriptions and intelligence visualization platforms are not supported by an operational framework, they result in a reactive security posture rather than an active defense mindset.

A robust operational framework make certain that security operations are mature enough to ingest relevant intelligence and enables timely actions. Such a framework would need to include more than technological maturity, but also processes and governance that are addressed when an organization invests in developing an internal intelligence capability, rather than only purchasing external intelligence mechanisms. However, in many organizations these framework considerations are often passed over or are insufficiently developed to keep up with a dynamic, ever-changing threat landscape.

One of the primary constraints organizations face when considering a mature CTI capability is cost. Developing a robust intelligence capability can be expensive, and purchased services such as subscriptions and intelligence platforms come with their own set of challenges. For example, these types of services are often tailored toward a technical audience and lack industry focus — this poses a challenge for executives who require business risk-centric analysis on industry-specific threats that can be leveraged for strategic planning.

Subscriptions

A CTI subscription provides access to malicious Web/URL, command and control, and malware data feeds. In order to provide value, the intelligence must be actionable and incorporated directly into security policies to actively block intrusions.

Subscriptions should be customized to the industry and the organization's needs in order to enable actions. This can be achieved by the provider working with the organization to determine the right selection of subscription offerings, which can be a combination of the following:

- Tailored technical indicator feeds for automatic integration
- Informative webcasts and training events to target the operationalization of threat intelligence
- Analyst-delivered briefings to inform both security operators and executives
- Industry- and business-specific reporting on current events, emerging cyber threats and trends on customized time schedules to meet operational needs (daily, weekly, etc.)
- Timely event-driven updates with analysis on significant and relevant cyber events

Having direct analyst support to deliver products, provide briefings, answer intelligence-related questions, and tailor analysis and recommendations to an organization's threat landscape is pivotal for maximizing the use of subscription services.

Intelligence platforms

Intelligence platforms can be a crucial component to cybersecurity when combined with key processes within a mature intelligence program to visualize collected data and support long-term trending. Trending analysis can provide valuable insight specific to the organization and to industry by showing changes in adversary tactics, techniques and procedures (TTP) over time, and patterns in intelligence of value determined when key stakeholders take the time to document their intelligence requirements. This analysis is most effective when captured in a way that leaders find meaningful to business risk decision-making and the prioritization of countermeasures and remediation activities.

CTI market development

The development of mature CTI programs within a cybersecurity framework is the natural evolution of threat intelligence services beyond purchased subscriptions, feeds and technical platforms. It is a long-term investment, which requires dedication and key stakeholders that can realize the lasting benefits

this type of service provides. These long-term visions among stakeholders are emerging despite conducting business in a world that promotes smaller immediate value to cybersecurity over growing a more mature and secure posture over time. Intelligence services of this kind include a customized approach to governance, people, processes, technology and data.

A robust CTI integration is grounded in tailored assessments that answer specific stakeholder questions, consider the organization's unique threat landscape, and provide immediate operational value with thorough recommended actions. To support this, organizations should consider developing a CTI program and also conduct a periodic assessment of how the threat landscape might affect them.

CTI programs

A CTI program provides an organization's security operation the ability to collect, analyze, produce and integrate its own and external intelligence. The design, build and operations development of a CTI program supports simultaneous growth within corresponding security operations, allowing the organization to process increasingly more robust threat intelligence, subsequently keeping the business from being overwhelmed by data.

CTI assessments

The marketplace has gaps between an organization digesting threat intelligence and an organization integrating the intelligence into operations. A common theme is frustration with where to start. CTI can be implemented incrementally, allowing small investments to improve and mature other areas of cyber threat management in a way that maximizes return on investment.

Tailored assessments gather the pertinent facts and organize the pros and cons of various program attributes to promote a process-oriented approach, providing immediate insights and an evaluated look at where organizations can start integrating CTI. These assessments can answer specific business questions, providing a clear way forward through recommendations.

Operationalizing CTI

A common challenge that permeates the industry is how best to make use of CTI:

- How can an organization go about making CTI relevant and actionable?
- How can an organization integrate relevant and actionable intelligence into security operations?

Only through unearthing an organization's unique CTI requirements and designing custom integration processes can the organization truly operationalize CTI.

However, several issues may exist that limit the operationalization of CTI:

- Lack of consolidation of intelligence sources (i.e., multiple subscriptions owned by the organization used by different divisions and not shared)
- An inability to properly integrate purchased intelligence feeds into security technologies, which limits the ability to use the intelligence purchased in a meaningful way

The future of CTI

Despite CTI not being fully adapted within the marketplace, organizations will need to continue to adapt to change in the cyber threat landscape to better understand how threat intelligence can reduce their overall business risk. CTI discussions surrounding business risk rather than just security risk will become more and more common. Understanding cyber threat risks to the business's finances, reputation, information, and operations will continue to broaden the discussion beyond a security or technology audience.

Short-sighted and pressured organizations will continue to buy threat intelligence feeds and technologies, without aligning such investments to a long-term vision for governance, integrated processes and unique business requirements. However, more and more companies will begin focusing on building a robust threat intelligence capability and/or using tailored intelligence to answer their

specific business questions. This will lead to greater investments in the process design surrounding CTI and industry/organization tailoring of threat intelligence.

Leading organizations will focus more heavily on customizing available CTI on their own and will become more willing to share threat intelligence with others in their ecosystem in order to make the threat intelligence actionable. In turn, CTI vendors will need to become more focused on providing details on how the adversary operates (dynamic indicators) than on sharing singular indicators of compromise (static indicators) that lack context.

Industries with increasing risk and unique challenges, such as oil and gas, retail, health care, food and agriculture will increase investment in the area of CTI and, as these industries continue to evolve their threat intelligence capabilities, they will undoubtedly contribute to the further development of the best practices in cybersecurity.

CTI will help to enable organizations to leverage next-generation security concepts such as threat modeling, active defense and advanced countermeasure operations. The purpose will be to develop repeatable processes that are effective for all organizations in transitioning from a reactive security posture to a proactive approach. Organizations will better appreciate the need for understanding their own environment at a much deeper level in order to achieve this.

There will be increased investment in the detailed mapping of networked environments, the long-term storage and visualization of security operations data, the identification and valuation of high-value assets, governance and process design surrounding currently siloed security capabilities, the war-gaming of cyber scenarios against such assets, and the testing of countermeasures.

Risks and threats change over time. CTI processes can help organizations keep ahead of threats, mitigate risks, and ultimately guarantee the success of the organization.

5. Cyber supply chain risk management

EY recommends the following updates to the Framework's Supply Chain Risk Management (SCRM) section.

In general, the addition of SCRM to the Framework appears to be inconsistent with previous NIST guidance. As an example, SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, 2015, identifies risk management process steps as "Frame, Assess, Respond, and Monitor" and risk responses as "Accept, Mitigate, Share, Transfer, Avoid." The Framework refers to risk management processes as "Identify, Assess and Mitigate" (page 10).

There also needs to be a greater emphasis on fundamentals, such as accountability, ownership, contractually enforceable monitoring service or product performance, establishing alternatives (Plan B), and processes for appropriate sunsetting (e.g., data destruction).

Another example occurs with the addition of SCRM to the Implementation Tiers. SP 800-161 notes, "ICT SCRM should be integrated into the organization-wide risk management process …" (page 16). NIST Framework Version1.1 notes, "Enterprise risk management is the consideration of all risks to achieving a given business objective" (page 10). Adding SCRM to the tiers as a separate, parallel risk management type detracts from NISTS's previous messages that 1) enterprise risk management is the consideration of all risks; and 2) SCRM should be integrated into the organization-wide risk management process.

Regarding the architecture of the Core, all new SCRM processes were added in one place — Supply Chain Risk Management (ID.SC) — opposed to integration based on the primary activity required to implement the control. For example, the primary activity to implement the following control is response and recovery planning: "ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers." The usability of the Framework would be lessened by forgoing a control activity based implementation taxonomy that is used for the current, non-SCRM subcategories. We believe that these revisions will help Framework users implement cybersecurity controls and achieve

results outlined in the "Subcategory" section, thereby improving the cybersecurity posture of the organization.

SCRM can be further enhanced with measuring and demonstrating cybersecurity.

EY believes that incorporating SP-800-55 (R1)'s quantifiable measurements will help demonstrate and determine cyber program efficacy.

6. Additional observations

EY also made the following observations:

A. EY recommends adding a built-in mechanism to assess cost-effectiveness. Lack of cost data makes it very difficult for Framework implementers to understand successful and less successful cyber topics. The recently signed American Innovation and Competitiveness Act (01/06/2017), Section 104 (Cybersecurity Research) states that NIST shall conduct research and analysis to:

    1) Determine the nature and extent of information security vulnerabilities and techniques for **providing cost effective information security**" (emphasis added)

    2) Review and determine prevalent information security challenges and deficiencies … **that may undermine the effectiveness of agency information security programs and practices** (emphasis added)

    3) **Evaluate the effectiveness,** sufficiency and challenges to federal agencies' implementation of standards and guidelines (emphasis added)

B. Currently, not all of the Framework's informative references are mapped to SP 800-53 (R4), making it difficult to support that the Framework has been fully baselined to the *de facto* cybersecurity standard. We recommend that all of the Framework's informative references be mapped to SP 800-53 (R4) controls.

C. The Framework is intended for critical infrastructure, but does not reference the Industrial Control System (ICS) controls listed in SP 800-82 (R2), Guide to Industrial Control Systems (ICS) Security. The usability of the Framework within critical infrastructure environments would be improved with the incorporation of references to ICS controls found in SP 800-82 (R2).

D. Usability of the Framework would be improved through further alignment with risk management practices included in SP 800-37 (R1), Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, 1 February 2010. Examples include:

    1) Avoid security/technology focus

    2) Identify mission critical business processes

    3) Map the assets that support mission critical business processes

    4) Assess assets to understand inherent risk exposure

E. Information Technology (IT) and Operational Technology (OT) are often referenced, but not defined. Within the marketplace, organizations have a difficult time defining IT vs. OT, especially as these systems converge. Unnecessary confusion may be avoided by defining IT and OT assets in the Framework and denoting an applicability (IT vs. OT) for subcategories within the Framework's Core. By inserting an applicability section within the Core, users of the Framework would have a better understanding if specific subcategories and related informative references apply to OT assets or if only a select set of subcategories and informative references apply to OT assets.

F. The Core currently provides an approach that does not take into account the criticality of the business processes that an organization's IT and OT assets support. The Core provides a minimum set of subcategories that an organization should consider for implementation, but does not offer an approach for organizations to tie critical business processes to supporting IT/OT assets and applying subcategories in a prioritized approach. We recommend that the Framework be updated to include a clear, concise methodology that lays out a prioritized implementation approach for organizations based off of risk and criticality.

G. The Framework is supposed to be more foundational or baseline in nature but misses or underserves some key cyber risk management domains or practices.

H. The Framework could better explain risk management practices that create the foundation for identity access management and control. There seems to be a lack of emphasis on fundamental objectives, such as least privilege, need to know and separation of duty.

I. There needs to be more of an emphasis on key risk indicators that form the basis to evaluate cyber program performance.

J. The Framework should direct the user to analyze the risk/impact of security controls and help identify the impact level (high, moderate or low) of the measures being considered.

Closing

EY thanks NIST for the opportunity to provide feedback on Framework Draft Version 1.1.

References

1. American Innovation and Competitiveness Act, 6 January 2017.
2. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, 12 February 2014.
3. Framework for Improving Critical Infrastructure Cybersecurity, Draft Version 1.1, 10 January 2017.
4. How do you find the criminals before they commit the cybercrime? A close look at cyber threat intelligence, EY, 2016.
5. SP 800-37 (R1), Guide for Applying the Risk Management Framework to Federal Information Systems, 1 February 2010.
6. SP 800-53 (R4): Security and Privacy Controls for Federal Information Systems and Organizations, 1 April 2013.
7. SP 800-55 (R1), Performance Measurement Guide for Information Security, 1 July 2008.
8. SP 800-82 (R2), Guide to Industrial Control Systems (ICS) Security, 1 February 2015.
9. SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, 1 April 2015.

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

1410-1336418

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com