EO 13636: Improving Critical Infrastructure Cybersecurity

New frameworks, information sharing, and risk-based processes

"Enemies of the US want to sabotage the country's power grid, financial networks, and air-traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."

—US President Barack Obama

Executive Order Timeline

The order includes timing for the creation and adoption of its key components. One of the major elements that will affect CI security planning and architecture discussions is the NIST Cybersecurity Framework. It is slated to be completed by February 2014, 12 months after the EO was issued.

Introduction

Citing repeated cybersecurity breaches into critical infrastructure (CI) and growing cyberthreats, in February 2013 the White House issued Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity. Now, several months later, federal agencies, industry partners, and owners and operators of critical infrastructure have made steady progress toward the EO's goal to enhance the security and resiliency of US critical infrastructure.

The EO directs federal agencies—including the National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), and Department of Defense (DoD)—to create a partnership with the owners and operators of critical infrastructure to address cyberthreats through:

- Development of a cybersecurity framework.
- New information sharing to provide classified and unclassified threat and attack information to US companies.
- A voluntary program to promote the adoption of the framework.
- Review of existing cybersecurity regulation.
- Strong privacy and civil liberties protections based on the Fair Information Practice Principles.

The EO encompasses a wide range of organizations as critical infrastructure, such as energy, healthcare, and financial services. This breadth of coverage results from interdependencies between systems. Cybercriminals and cyberterrorists attack the weakest point in a chain—and there are many links in the supply and process chains that enable America's security, national economic security, national public health, and safety.

This solution brief describes the core EO activities, progress to date, and McAfee contributions toward the success of this initiative. It should help affected entities—owners and operators of critical infrastructure—participate in the process, drive positive incentives rather than punitive regulations, and show innovation in securing these crucial systems.

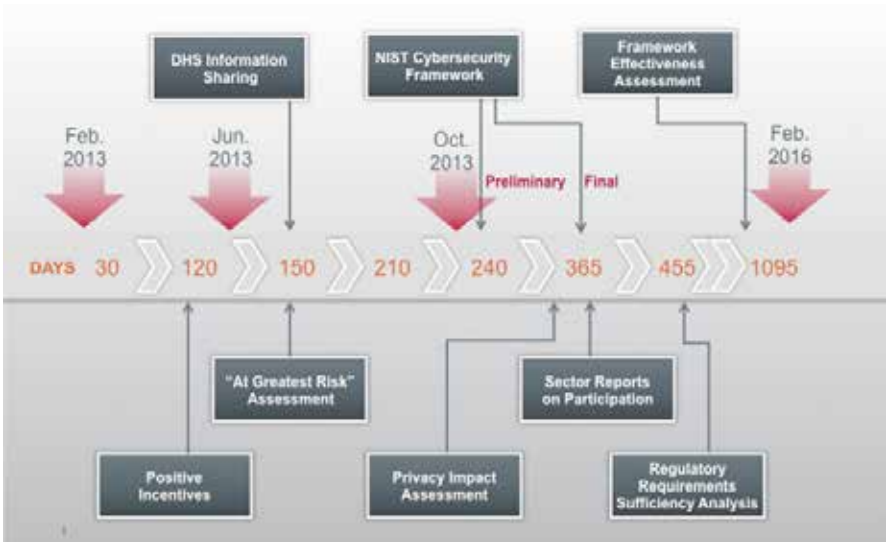

Figure 1. The EO includes a detailed timeline of deliverables.

Critical Infrastructure Sectors

As part of the EO, the DHS Secretary identified CI sectors. The EO defines CI as "systems and assets, whether physical or virtual, so vital to the [US] that the incapability or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

CI sectors include:

- Chemical.
- Commercial facilities:
  - Critical manufacturing.
  - Defense industrial base.
  - Energy.
- Communications.
- Dams.
- Defense industrial base.
- Emergency services.
- Energy.
- Financial services.
- Food and agriculture.
- Government facilities.
- Healthcare and public health.
- Information technology
- National monuments and icons.
- Postal and shipping.
- Nuclear reactors, materials, and waste.
- Transportation systems.
- Water and wastewater systems.

The most at-risk entities identified as of fall 2013 include financial services, telecommunications, and energy. Using the current National Infrastructure Protection Plan (NIPP) framework, which pairs subject matter experts and policy experts within the government and private companies for each sector, agencies are conducting sector-specific risk self-assessments to determine if current cybersecurity regulatory requirements are sufficient.

Sector plans and risk assessments will provide input to the types of vulnerabilities that surface across "cyber" and kinetic infrastructures. These will be addressed in the cybersecurity framework to enable continuous identification and remediation of these vulnerabilities to achieve increased infrastructure resilience across sectors. This is the same concept as the Continuous Diagnostics and Mitigation (CDM) used in government networks, which recommends network components learn as they protect and share information in near real-time within the network and across networks to create the resilience over time that mirrors a biological immune system.

Fall 2013 Updates

Since the issuance of EO 13636, federal agencies and industry partners have made steady progress across many of the EO components.

Cybersecurity framework

NIST is working in collaboration with the private sector and owners and operators of critical infrastructure to draft a proposed framework. NIST will then spearhead adoption efforts for the cybersecurity framework.

Figure 2. The NIST framework proposes use of a visual profile of an operator's risk management in five core functions. Tiers represent progress toward an "adaptive" level of risk management.

NIST is on target to publish the draft framework in October 2013. Based on request for information (RFI) responses and conclusions from a series of workshops, in August NIST submitted a discussion draft of the preliminary cybersecurity framework. It proposes that the framework consist of three parts:

- Framework core

  A compilation of cybersecurity activities and references that is common across critical infrastructure sectors. The core presents standards and best practices that allow for communication and risk management across the organization and consists of five functions that can provide a high-level, strategic view of an organization's management of cybersecurity risk, including:

  – Identify.
  – Protect.
  – Detect.
  – Respond.
  – Recover.

- Framework implementation tiers

  The tiers demonstrate the implementation of the Framework Core Functions and Categories and indicate how cybersecurity risk is managed. The tiers range from partial (tier 0) to adaptive (tier 3) with each tier building on the previous.

- Framework profile

  A profile conveys how an organization manages cybersecurity risk in each of the Framework Core Functions and Categories by identifying the subcategories that are implemented or planned for implementation. Profiles are also used to identify the appropriate goals for an organization or for a critical infrastructure sector and to assess progress against meeting those goals.[1]

Another notable recommendation from the workshop discussions is the desire to create a third-party moderator function to provide management, oversight, and improvement of the final framework going forward. The goal would be to provide CI sectors the greatest resiliency and effectiveness in implementing the framework without the need for regulatory controls.

Information sharing

Where today agencies share threat information within the public sector, DHS and DoD are working to establish procedures for an Enhanced Cybersecurity Services initiative that will have the DHS provide detailed threat information to each targeted CI entity.

Information sharing between the government and the private sector—and between private sector entities themselves—can be a powerful tool to thwart cyberadversaries. Threat information, such as event data, machine data, URL and risk reputation levels, network traffic patterns, and infection patterns, will improve and speed detection, understanding, forensics, and event resolution. Use of the threat information is voluntary, but details on each organization's responses will be reported back up to the president annually by sector-specific agencies. This visibility is intended to encourage participation. DHS and DoD are working to establish procedures for this initiative.

Positive incentives

The administration continues to embrace positive incentives, defined as "a cost or benefit that motivates a decision or action by critical infrastructure asset owners/operators to adopt the cybersecurity framework under development by NIST." Reflecting the input of each participating Sector Council, the US Department of Homeland Security, Commerce, and the US Department of the Treasury have submitted to the White House a set of positive incentives designed to promote voluntary adoption of the framework.

In addition, a voluntary program comprised of a public-private partnership will be created after the final framework is released in February 2014 to monitor and manage the effectiveness of positive incentives in encouraging framework adoption.

The recommendations balance cybersecurity benefits against the cost of framework adoption. The positive incentives garnering the most support are those anticipated to generate the highest efficiencies and cybersecurity effectiveness with the lowest cost incurred by the participating critical infrastructure sectors, consumers, and the government, including:

- *Cybersecurity insurance*—Engages with the insurance industry to build underwriting practices that promote the adoption of cyberrisk-reducing measures and risk-based pricing and foster a competitive cyberinsurance market.
- *Grants*—Suggests incentivizing the adoption of the framework as a condition or as one of the weighted criteria for federal critical infrastructure grants.
- *Process preference*—Includes a range of government programs in which adoption of the framework could be considered in expediting existing government service delivery. For example, outside of emergency situations, the government could use framework adoption and participation as secondary criteria for prioritizing who receives that government-provided technical assistance.
- *Liability limitation*—Possible legislation to reduce liability on framework participants to encourage adoption, including reduced tort liability, limited indemnity, higher burdens of proof, or the creation of a federal legal privilege that preempts state disclosure requirements.
- *Streamline regulations*—As the framework and voluntary program are developed, agencies will recommend other areas that could help make compliance easier, for example, eliminating overlaps among existing laws and regulation, enabling equivalent adoption across regulatory structures, and reducing audit burdens.
- *Public recognition*—DHS will work with the critical infrastructure community to consider areas for optional public recognition as they work together to develop the framework.
- *Rate recovery for price-regulated industries*—Enables recovery of cybersecurity investments within the rate base charged for services provided by framework owners and operators. Further investigation is required to determine the viability of this possible positive incentive.
- *Cybersecurity researc*h—Emphasizes research and development to meet the most pressing cybersecurity challenges where commercial solutions are not currently available.

While this list does not represent a finalized plan, it does offer an initial look at how CI entities could be incentivized to adopt the cybersecurity framework as envisioned in the EO.

McAfee Provides an Industry Voice

McAfee has been active on several fronts. Our goal in working with the administration is to help ensure that rules and implementation timelines are created and rolled out in a manner that ensures our customers can innovate without the burden of excessive regulations.

McAfee is part of the Information Technology Sector Coordinating Council (IT-SCC), which is one of the 18 coordinating sectors that have provided input to the DHS incentives process. We are also closely involved with the NIST cybersecurity framework's development. For example, when NIST released their RFI asking industry and other stakeholders for input on how they manage cybersecurity risk, what international standards they use, and what methods and technologies they have in place to protect their systems, McAfee submitted a lengthy RFI response. We have also dispatched a contingent of architects to the series of NIST workshops that have led up to the draft framework of October 2013.

Our goal through this participation is to ensure that NIST engages with the private sector in a strong, but flexible and truly voluntary process. We are recommending that internationally accepted industry standards form the foundation of any frameworks, approaches, or standards proposed by NIST. We are pleased to see that the preliminary draft's framework core is comprised of international, national, and community best practices as information references, such as the top 20 critical controls from the Council on Cybersecurity (CCS), and that it can be extended and customized to suit an organization's specific risk management processes and organizational constraints.

The Role of CI Owners and Operators

The cybersecurity threat to the US critical infrastructures is real. EO 13636 gives CI owner operators an opportunity to be proactive and get engaged in shaping a modernized, viable framework that addresses this growing risk. Collaborative participation from members of the CI community demonstrates to federal agencies that voluntary initiatives are possible and do work—especially as compared to punitive-style regulations, which tend to inspire the bare minimum to meet compliance requirements.

McAfee is representing its customers and the industry as actively and vigorously as possible. We are also committed to ensuring that McAfee solutions continue to innovate according to the unfolding framework's recommendations. However, for the effort to have the most positive outcomes, it is crucial that affected entities also raise their voices and take proactive steps such as:

Provide your feedback

CI owners and operators can get involved and provide NIST with feedback on the discussion draft of the preliminary cybersecurity framework.

Assess your risk posture

Make sure you have reviewed the *CERT Cross-Sector Roadmap for Cybersecurity of Control Systems* document to understand the security controls most important to Critical Infrastructure Protection (CIP).

Figure 3. Target profile creation process.

Assess your current risk posture

See where you stand today. The NIST framework includes guidance on how to establish or improve a cybersecurity program using a risk management process and a target profile. The Critical Infrastructure Security Assessment service is available from McAfee® Foundstone® consulting services. McAfee partners can also help provide insight into your current risk posture, security inventory, available data feeds (such as threats and events), and weak spots. Through early understanding, you have time to build out your plan to address any shortcomings—areas where your current profile falls below the target profile. For example, some sectors will find they have prioritized safety or reliability over security. Yet all three are necessary and interrelated components of a resilient infrastructure. CI entities should be clear that security can enhance safety and reliability through improvements to availability and integrity.

Weigh and mitigate cybersecurity risks

An essential tenet of risk-based security management is that not all risk can or should be mitigated. The August 28, 2013 NIST discussion draft of the preliminary cybersecurity framework states: "Some actions, such as 'Inventory and track physical devices and systems within the organization.' are basic and necessary for practically all organizations. Other actions are potentially more costly and are usually only implemented when a risk assessment indicates that they are necessary."

Some risk should be accepted if the mitigation costs more than the benefit in risk reduction. Once you understand your risk posture, you can use asset values, threats, and countermeasures already in place to decide how and where to invest in risk mitigation. To help you close these protection gaps, McAfee offers a complete platform of endpoint, network, and data protections integrated through a common security management environment. These solutions—and more than 100 integrated partners—can help you deploy and maintain appropriate countermeasures where they will be most effective.

Continuously monitor risk

Every cybersecurity program requires continuous visibility into what is happening across enterprise IT, SCADA, and ICS networks. NIST describes continuous monitoring of CI risk levels as a key component of a comprehensive security plan, which is one that shifts the emphasis to a more automated and proactive model. You should review your environment to see how well your monitoring systems inform you of ongoing changes to your risk posture.

As a way of operationalizing risk management, CI owners and operators may want to deploy security and compliance tools such as McAfee Risk Advisor, McAfee Vulnerability Manager, McAfee Policy Auditor, and McAfee Enterprise Security Manager. These tools facilitate continuous monitoring of assets, threats, and vulnerabilities and can provide new insight into your organization's day-to-day risk, including visibility across actions and events on enterprise IT, command and control, and embedded networks. Updated threat feeds from the McAfee Global Threat Intelligence network and McAfee Labs researchers help McAfee products maintain essential risk intelligence to automatically block emerging threats.

Learn More

Protecting critical infrastructure is about a comprehensive approach—not a single product. The good news is that McAfee has proven experience securing critical infrastructure entities with our Security Connected framework that enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. McAfee empowers organizations to address cybersecurity threats proactively while maintaining availability across IT, SCADA, and ICS infrastructure. We have leading security services and solutions that enable you to assess your current CI risk posture, mitigate the full spectrum of threats, and continuously monitor and manage your risk.

For more information on how McAfee can help you adopt risk-based processes and secure your critical infrastructure, please contact us or visit:

- McAfee Critical Infrastructure Resources
- McAfee Public Sector Resources

[1] Descriptions excerpted from the *NIST Discussion Draft of the Preliminary Cybersecurity Framework, August 28, 2013.*

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60588brf_ci-cybersecurity_1013_fnl_ETMG