Cyber Security

Intel® Corporation

U.S. Executive Order 13636 and Critical Security Capabilities to Consider

White Paper

Authors

Amit Agrawal (Security Strategist, Intel)

Jack Lawson (Director - Security, Intel)

March 2014

Acknowledgements

Initiated and released by the Intel Corporation, this document was developed with support from across the organization and in direct collaboration with the following:

Editor

Steve Grobman (CTO, McAfee & Intel Security Group)

Key Contributors

Kevin Fiftal (*Intel*)
Michael Seawright (*Intel*)
Lorie Wigle (*McAfee*)
Jim Sarale (*McAfee*)
Tim Casey (Intel)
Kent B Landfield (McAfee)
John S Miller (Intel)
Dave Munsey (Intel)
Brian Willis (Intel)
Claire Vishik (Intel)

Feedback

Please send comments or suggestions about this document to the author at amit.s.agrawal@intel.com.

Executive Summary

On February 12, 2014, the Obama Administration announced the launch of the Cybersecurity Framework ("Framework"). The Framework was developed through a year-long effort, led by the National Institute of Standards and Technology (NIST) to gather private sector input on a voluntary, how-to guide for public and private sector critical infrastructure organizations to enhance their cybersecurity. The Framework is a key deliverable from Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity*[1] that President Obama announced in his 2013 State of the Union Address.

The Framework provides a guide to help organizations understand, communicate, and manage their cyber risks. In addition, the Framework provides a mechanism for gathering and organizing existing global cyber security standards and best practices. For organizations that do not know where to start, the Framework provides a road map. For organizations with more advanced cybersecurity, the Framework offers a way to better communicate with their CEOs and with suppliers about management of cyber risks. Organizations outside the United States may also choose use the Framework to support their own cybersecurity efforts.

Each of the Framework components reinforces the connection between business drivers and cybersecurity activities. The Framework also offers guidance regarding privacy and civil liberties considerations that may result from cybersecurity activities.

- The Framework Core is a set of cybersecurity activities and informative references that are common across critical infrastructure sectors. The cybersecurity activities are grouped into five functions—Identify, Protect, Detect, Respond, and Recover—that provide a high-level view of an organization's management of cyber risks.
- The Profiles can help organizations align their cybersecurity activities with business requirements, risk tolerances, and resources. Companies can use the Profiles to understand their current cybersecurity state, support prioritization, and to measure progress towards a target state.
- The Tiers provide a mechanism for organizations to view their approach and processes for managing cyber risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigor in risk management practices, the extent to which cybersecurity risk management is informed by business needs, and its integration into an organization's overall risk management practices.

The U.S. economy relies heavily on information technology (IT). All of the sectors in a nation's critical infrastructure have IT infrastructure upon which many of their operations function. Most organizational processes today are electronic and depend heavily on both security technologies and an informed understanding of security risks. Although considerable progress has been made toward improving infrastructure security capabilities, more can and should be done. Today, all critical infrastructure relies on digital systems of computation and communication, often collectively referred to simply as "cyber." Critical infrastructure providers must be proactive in managing cyber risk created by an evolving and increasingly sophisticated set of external adversaries, from individual hackers to organized criminal groups to nation states, as well as insider threats. Cyber risk impacts a company's bottom line,

similar to financial and reputational risk. It can harm a company's ability to innovate, to gain and maintain customers, and can drive up costs and negatively impact revenue.

Use or adoption of the Framework by organizations is voluntary. NIST and industry together will continue to update and improve future versions of the Framework as industry provides feedback on its utilization. At Intel, we believe understanding and utilizing the Framework are important not only to the express goal of increasing the cybersecurity of critical infrastructure but to the future success and safety of our customers.

Intel has been actively engaged with NIST through public workshops that were held to develop the Framework and will continue to contribute to the future maturation of the Framework and its governance. Intel's recommendation is that organizations utilize the Framework to better understand and manage their cyber risk through a security approach grounded in multiple key security capabilities.

Goal of this White Paper

This paper provides background on the Framework and how the Framework can help organizations identify risks and mitigate those risks in their business. It also identifies a number of Intel's security capabilities, and explains how our customers can utilize these capabilities to mitigate their risks.

The risks described include those resulting from the emerging "Internet of Things" (IoT), on which critical infrastructure increasingly depends. Intel security capabilities target the devices and services essential to the IoT, and can play a key role in developing risk mitigations in alignment with the Framework.

One intent of the Executive Order and the Framework is to inspire a continuing dialogue around creating a more resilient cyber infrastructure within our nation's critical infrastructure. We look forward to continuing this dialogue around the Framework and connecting it to Intel's security capabilities to better inform discussions with our customers, industry partners, fellow travelers, and thought leaders. We believe as we start this dialogue and foster "best practices" discussions, all critical infrastructure providers will benefit.

Overview of Executive Order 13636

Executive Order 13636 – *Improving Critical Infrastructure Cybersecurity* arose from the Administration's belief that the cyber threat to critical infrastructure "continues to grow and represents one of the most serious national security challenges [the nation] must confront." The Executive Order focuses on improving information sharing on cyber threats with the private sector, ensuring the protection of privacy and civil liberties and creating a "Baseline Framework to Reduce Cyber Risk to Critical Infrastructure" and a voluntary program to support the Framework's adoption by critical infrastructure owners and operators and other interested parties.

President Obama called for this Framework to incorporate industry best practices and voluntary consensus standards. The Executive Order strove for a Framework consistent with voluntary international standards "when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act." It is important to note that the Framework did not introduce new standards, but instead highlighted existing voluntary standards already in use that met the objectives of the order. EO 13636 ordered the Framework to help owners and operators of critical infrastructure identify, assess, and manage cyber risk by providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls.

The Framework's objective is to help organizations manage their cyber risk by applying the principles and best practices of risk management to improve the security and resilience of critical infrastructure. The Framework offers a "road map" that allows organizations—regardless of size, degree of cyber risk or cybersecurity sophistication—to determine their own current level of cybersecurity, set goals for cybersecurity that are in sync with their business environment and establish a plan for improving or maintain their cybersecurity.

The U.S. Cybersecurity Framework

Under the direction of EO 13636, NIST's Cybersecurity Framework[2] addresses cybersecurity by:

- Identifying security standards and guidelines that are applicable across sectors of critical infrastructure, while also identifying areas that should be addressed through future collaboration with particular sectors and standards-developing organizations;
- Providing a prioritized, flexible, repeatable, performance-based, and cost-effective approach;
- Helping owners and operators of critical infrastructure identify, assess, and manage cyber risk;
- Providing guidance that is technology neutral and enables critical infrastructure sectors to benefit from a competitive market for products and services;
- Including guidance for measuring the performance of implementing the Framework;
- Including methodologies to identify and mitigate impacts of the Framework and associated information security measures or controls on business confidentiality, and to protect individual privacy and civil liberties.

The Framework embraces a risk-based approach to managing cybersecurity risk and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the Framework Profiles. Each Framework component reinforces the connection between business drivers and cybersecurity activities.

The Framework Core is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of

cybersecurity activities and outcomes across the organizations from the executive level to the implementation/operations level. The Framework Core consists of five concurrent and continuous Functions: Identify, Protect, Detect, Respond, and Recover. (See *Table 1.*) These Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

The Framework Implementation Tiers illustrate how an organization views cybersecurity risk and the processes in place to manage that risk. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework. The Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed. An organization does not necessarily strive to achieve Tier 4; the desired Tier is based on the evaluation of an organization's risk tolerance.

A Framework Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" Profile (the "as is" state) with a "Target" profile (the desired state). The Current Profile can be used to support prioritization and measurement of progress toward the Target Profile, while evaluating other business needs including cost-effectiveness and innovation. Profiles can be used to conduct self-assessments and communicate within an organization or between organizations.

One objective of the Framework is to provide organization and structure to multiple, complementary, and uncoordinated approaches to cybersecurity. The Framework provides tools to apply the principles and best practices of risk management to improving cybersecurity and securing critical infrastructure. By providing a common structure for defining an organization's cybersecurity profile, the Framework can support an organization in identifying and understanding an organization's dependencies with business partners, vendors, and suppliers.

The Framework is intended to support existing risk management processes by assembling standards and approaches that are working effectively in industry today. The Framework is designed to enhance the risk management approach an organization currently uses; and, if an organization does not have an existing risk management process, the Framework provides a foundation for building one. The Framework has created to tools to help an organization align its cyber risk profile with business partners along its supply chain and enable these partners maintain a cyber risk approach consistent with the delivery of critical infrastructure services.

The Framework is not a one-size-fits-all approach to managing cyber risk for critical infrastructure. An organization's risk is unique—different threats, different vulnerabilities, different risk tolerances—and the level of Framework implementation will vary. In addition, the Framework is designed to provide a common language to address and manage cyber risk as a mission equal in priority to other risk areas, such as financial and reputational risk, a company must address.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 1: Framework Core Functions[2]

An International Context for the Framework

Although the NIST-driven Framework was initiated and developed in the U.S., the initiative relies on international standards produced by the international community of technologists using an open standards development process, and was largely informed by private sector companies operating internationally. Pioneering national cybersecurity strategies developed in Germany, UK, and France focus on similar approaches as the Framework, and also provide views complementary to the Framework.

The Framework has become a reference point in defining practical approaches to cybersecurity infrastructure that, in the developed world, is mostly enabled by private industry. Thus, although practical application of the Framework enablement outside of the U.S. need to be studied, we believe that the Framework and positioning of products that have features aimed at reducing cybersecurity risks have strong applicability outside of the U.S.

Intel's Critical Security Capabilities

Intel has developed a number of security capabilities that align well with the philosophy and principles underlying the Framework. They are identified and described here to increase awareness amongst our customers (and other interested organizations) of these capabilities and their availability for use.

The Framework is a powerful tool for organizations to utilize in their efforts to secure both their enterprise and their products. It guides the organization in understanding what systems and components it needs to manage and respond to cyber risks. How to implement those systems and components, however, is left to each individual organization to decide for itself. This ensures organizations can implement risk and security systems based on their own needs, enabling maximum flexibility and supporting innovation.

Recent cyber-attacks on many different companies—and covered widely by the international press—underscore the importance of a strong cybersecurity risk management program for every organization. Hackers and other cyber criminals are increasingly sophisticated, and frequently focus their attention on emerging trends and technologies like IoT, cloud, and big data. Critical infrastructure providers must move more quickly to protect their cyber and physical assets from these fast evolving attacks.

Recognizing the problems of cyber security and the need to continually improve in advance of the growing threats, Intel has long focused on enhancing the security of the computing experience across the global digital infrastructure and for everyone using the Internet. Intel has engaged with its subsidiaries and partners to develop powerful capabilities that enhance the security of both Intel's products and those of our customers.

Most uniquely, Intel has incorporated security technologies that benefit from implementation in silicon or firmware. These technologies establish the hardened root of trust that is resilient to software-based attacks.

Intel believes hardware-based security is important to develop resilient products for Critical Infrastructure. Such approaches allow the technologists to build platforms with a comprehensive security approach. Using these available capabilities can help organizations meet their needs for faster and better cybersecurity risk management implementations.

Currently available Intel critical security capabilities, all of which align with the Framework, are briefly described below.

AVAILABLE CRITICAL SECURITY CAPABILITIES FROM INTEL

Hardware Root of Trust: All security is based on trust, and cybersecurity requires a reliable base where all trusted exchanges can originate: the root of trust. Many years of experience has shown that a hardware-based root of trust is robust and resilient to attack, and thus often is the most trustworthy. Intel believes security built into microprocessors and other chips is essential to cybersecurity and an approach we encourage others to emulate.

Encryption: Intel believes hardware-assisted encryption is an effective way to help protect sensitive data on the endpoint, to help meet stringent global regulations, protect personally

identifiable information, and minimize the risk of data breaches. Hardware-assisted encryption is a baseline capability that every device in the end-to-end chain should have.

Identity Protection: The frequency, severity, and ingenuity of cyber-attacks have increased. IT professionals, chief technology officers, and chief information officers are constantly seeking stronger techniques to protect the integrity of online business and financial transactions. Intel recommends the use of both hardware and software to help protect the identity of the platform and implement near seamless verification methods for users accessing such end devices.

Firewall: Intel envisions a unified and flexible security for every enterprise environment. Firewalls are an essential part of maintaining high availability and manageability, delivering advanced network protection across your entire enterprise. Firewall technology supports the security demands of data centers that need to deliver uninterrupted uptime with no gap in protection. A next-generation firewall includes behavioral tools that can analyze the data streams to identify known and suspected evasion techniques, increasing protection against advanced persistent threats (APT).

Manageability: Organizations must know the current state of the defense landscape at all times. A single, powerful management platform optimizes and centrally controls all of the devices in the information (IT) and operational (OT) sides of the corporate infrastructure and remote sites, making security management more efficient and lowering total cost of ownership. A central management system can define policies, and further can build and apply those policies for complex environments including physical and virtual devices without additional burden or complexity.

Trusted Pools: Virtualization management can identify and report platforms that demonstrate integrity and platform location. Robust security management software can allow identification of sensitive workloads and read platform trust status and location. This will allow the linkage of platform capability and location to workload classification via policy. Ultimately these policies can control virtual machines on platform trust to better protect data. Trusted pools allow for aggregation of multiple trusted systems and enable platform trust status as a data point for security applications to enforce control of workload assignments.

Boot Attestation: Secure boot uses root of trust to provide configuration verification useful in compliance. This technology can also enable domain isolation and tamper detection in boot process. It provides hardware-based security for a solid foundation for security starting from system power on. It provides a foundation on which a trusted platform can be built to protect against software-based attacks.

SIEM: SIEM (Security Information Event Management) enables best practice of three layers: common logging service, correlation layer, and predictive analytics. Such a security architecture provides scalability, and potentially compartmentalization for services across multiple customers. SIEM examines the distinct events together, looking for patterns in order to predict threat recognition. It can access the network for more information that may not be in logs, and is instrumental in protecting critical systems.

Intrusion: IPS (intrusion prevention systems) and IDS (intrusion detections systems), depending upon the environment, play an important role that will actively detect and analyze the network from an array of security attacks, including viruses, works, spyware and denial of service attacks. This technology becomes even more powerful when utilizing a relational data management engine, allowing IPS and IDS to identify threats and detect anomalies in real time, before they disrupt the network.

Whitelisting: Whitelisting is well-suited for fixed-function devices running only known, trusted software. Only permitted code registered on a carefully controlled list is allowed to execute, while unknown software is prevented from running. This is different from traditional blacklisting methodology such as antivirus software. Blacklisting solutions are ideal for situations in environments that can tolerate a high degree of user change, and where the signature files need to be updated constantly. In such environments, the user is exposed to bulk malware. The database of malware signature files in such situations needs to be updated almost on a daily basis for antivirus solutions to detect and remediate malware. Application whitelisting can provide a more effective solution, including effectiveness against zero-day attacks.

Input-Output Devices: Comprehensive device management helps control and block confidential data copied to removable storage devices. Also, similar such devices can be used to propagate malware into trusted devices. Local Access host controls (USB access, test ports, etc.) must be addressed and secured as well. Comprehensive device management can provide data protection by specifying detailed hardware and content-based filtering, monitoring, and blocking of devices connected to the systems. It can help deploy and manage security policy to prevent unauthorized devices getting connected to the system.

API Management and Security: As data usage grows, there are more applications than ever communicating with each other. API allows application functionality to expose data to partners. It allows application developers to automate interactions, resulting in increased collaboration. Due to wide spread use of APIs, it is necessary to deploy a best-in class API management and distribution platform that will provide a security service that treats sensitive data with extra caution. Such management layers allow system access that is strictly controlled and only permitted for those that have a need based on their role, thereby enforcing privacy protection throughout an organization’s operations.

Secure Update: Typically industrial and critical infrastructure controls are manually updated via commonly used removable media. This approach is error-prone as media can be mishandled, updates may be out-of-date, and bad actors can introduce malware that may defeat firewalls. Letting these updates pass through a firewall introduces security risk for many networks. Intel highly recommends the use of cryptographic signatures and tokens that allow for authentication of such updates, enabling them to pass through the firewall in a secure manner, while preventing installation and execution of unauthorized code. This is a good strategy as it hardens the devices for longer periods and opens extensibility for update capabilities which can be controlled by the customer

Isolation: To ensure the highest degree of security, it is critical to draw the line between the information (IT) and operational (OT) sides of the network. It must be assumed that any network connection will introduce security risks, especially if it can find a pathway to the Internet. Isolation of critical assets as part of a network protection strategy must be a fundamental principle of defense-in-depth. Risk management of assets is also very important, and imposing heterogeneous enclave security controls (network, process, SW, transport) at a rate on par with attackers' innovation can help.

Virtual Private Networks (VPN): Today's personal computing devices like laptops, tablets and phones have enabled easy access of the corporate information on personal devices. This situation is further complicated by use of Bring-Your-Own-Device (BYOD) model which has blurred the line as to what a corporate compute device is. Virtual Private Networks (VPN) allow for improved security when accessing resources on a network to which one is not physically connected. It allows the communication to be encrypted, which means that the data and applications are restricted to only who are authorized users. We encourage stronger VPN capabilities (secure, monitor, OOB manageability for recovery, etc.) for most of them to minimize risks to the critical data.

Hardened Operating Systems: One of the most common tools used by hackers is to modify an application or chain together vulnerabilities so it can run at the trusted level of an operating system. Intel recommends that operating systems implement mechanisms in hardware and/or software to prevent an entire class of escalation of privilege attacks on the operating system. This built-in security technology works constantly to deliver extensive, automatic "blanket" protection that defends against these sophisticated attacks and helps prevent rootkits and malware from taking deep hold in the system.

Summary

Intel's mission is to incorporate end-to-end security by enabling the ecosystem with best in class capabilities developed by security by design. We look forward to addressing our customer's security requirements by way of broader industry collaboration and our continued work with NIST. We encourage our customers and industry partners to join us in this dialogue and begin moving all forms of critical infrastructure to a more secure foundation.

References

1. *Executive Order 13636 – Improving Critical Infrastructure Cybersecurity*, The White House. Office of the Press Secretary. Feb 12, 2013. http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
2. *Framework for Improving Critical Infrastructure Cybersecurity Version 1.0,* National Institute of Standards and Technology. Feb 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf