Motorola Solutions—Experience with the Framework for Improving Critical Infrastructure Cybersecurity

Motorola Solutions (MSI) offers feedback to the National Institute of Standards and Technology (NIST) about the level of awareness and initial experiences with the Framework for Improving Critical Infrastructure Cybersecurity. MSI plays an important role for mission-critical communications and supports critical infrastructure in their ability to plan for, prevent, protect, respond to, and recover from all hazards, including man-made and natural incidents. Our participation with NIST in the development of the Cybersecurity Framework (Framework) underscored the collaborative approach for the establishment of industry-led standards, guidelines and best practices. We support the goal to create a conversation around cybersecurity as a component of the overall business risk management process and offer our experience in the application of the Framework to help guide future efforts.

MSI serves a global marketplace with over 10,000 systems deployed in more than 100 countries; Motorola Solutions is also an owner and operator of critical communications systems in support of public safety and emergency services globally. We have dedicated significant resources to protect our global enterprise information technology systems, as well as secure our product design, development, deployment, operations and maintenance functions. Motorola Solutions maintains a risk management process for identifying, assessing, and responding to risk, the Framework complements and does not replace our existing cybersecurity risk management program.

Our policies and practices were originally developed in the late 1980's as part of our formal Information Security Organization and receive continuing attention to enable information assurance best practices. These policies and practices receive reviews annually with updates implemented on a multi-year cycle or as needed due to changing circumstances. Our internal audit organization verifies information security policy modifications as well as adoption compliance within our businesses and customer facing products. Much of MSI's cybersecurity capability maturity is the direct result of increasing threats and the required operational response.

Clearly policy and political attention to cybersecurity continues to increase around the world to address a variety of threats from potential terrorism, to malicious programming and organized crime. The ever-changing cybersecurity landscape is a global issue and leads to questions about how to protect critical data and privacy both domestically and internationally. Cybersecurity in a global interconnected system that spans geographic borders and national jurisdictions needs globally accepted standards and assurance programs. We believe effective measures must be deployed across the entire global infrastructure. Simply put, the need to meet multiple, conflicting security and conformity assessment requirements in multiple jurisdictions is not practical. These efforts need to be dynamic and must adapt to emerging threats, technologies and business models.

U.S. policy has established roles and responsibilities for federal agencies to work with the private sector for enhancing the security of critical infrastructure. These public and private participants have a well established history of working together to protect critical physical assets; exercising these partnerships to protect cyber assets is well underway in the deployment of the Framework. From our experience, the level of awareness of the Framework is complete within this select community of critical infrastructure owners and operators—the private sector entities that participate with the federal government's risk assessment process in the identification, prioritization and protection of the critical infrastructure.

However, beyond this owner/operator community, the cybersecurity "ecosystem" consists of an expanded group of interdependent participants, such as: suppliers and consumers, users and devices, providers, access networks, core networks, infrastructure providers, and application and content providers. This interdependency "problem" is particularly challenging—the extension of the coordination mechanisms for planning and conducting risk assessments with an expanded community of interdependent participants is an important next step. Extending these capabilities will improve the physical and cyber security of sector assets; ease the flow of information within the sectors, across sectors; and address issues related to response and recovery to assure the continued operation of vital services. The federal government needs to work closely with the private sector to promote real-time information sharing between the public and private sector, in order to be able to react at internet speeds; this real-time information sharing capability must be more widely available and automated.

A key development is that customer expectations -- expressed both informally and formally -- are beginning to demand a more comprehensive approach to security throughout the solution development, implementation and operational lifecycles. In order to be a trusted supplier, there needs to be assurance that the system functions as intended and is free of exploitable vulnerabilities, either intentionally or unintentionally designed or inserted, at any time. As a supplier of mission critical systems, the integrity of our solutions reflects directly on our brand.

Potential changes to procurement rules are also creating interest in whether the Framework could lead to more trusted products and services. However, different policies are being adopted globally; encouraging "Buy National" behavior—supply chain integrity is an emerging issue that will impact supplier agreements and the overall risk management process. MSI's support of the Framework is driven by expectations for a common set of standards, procedures, and processes that align policy, business, and technological approaches to address these risks.

MSI's application of the Framework included interdisciplinary representatives from across the company to review the key functions of cybersecurity—identifying assets, put protections in place, detect breaches, respond to the breaches detected and finally recover and learn. Informative references (ISO/NIST) were on hand to assure a detailed understanding of the recommended standards. The process included a step by step review of the Framework's core functions, categories, and standards—resulting in a scoring of MSI's implementation across the recommended security controls. To facilitate the process, a "tool" was developed that included the functions, categories and informative references that allowed for participants to assess the implementation levels for both the current and target profiles. The detailed definitions of the Implementation levels were also on hand to make sure there was a consistent measurement throughout the process.

Motorola Solutions identified our business related systems and assets and based on our risk approach, created a profile that reflects our current cybersecurity capability and implementation. The result was a profile, or a "score" across the core functions—identify, protect, detect, respond and recover. The Framework includes rankings on a scale from 1 to 4 (low-high) that provide an indicator and measure of capability maturity. As we conducted our assessment, we analyzed our operational environment, the likelihood of a cybersecurity event and the impact on our organization and established a score for each of the controls. Not surprisingly, MSI has a well-established and repeatable cybersecurity capability; our efforts are dynamic and are based upon a constantly evolving risk management process. We have transitioned from dependence on external intelligence to reliance on internal intelligence, including increased security protections by increasing user education and awareness, and preventing exploitation through intelligent analysis and triage of security events.

During the process and in response to the gaps identified in our Current Profile we developed action plans and created a Target Profile aimed at our organization's desired cybersecurity capability. There remains the challenge to fully incorporate the assessment findings into executive level decision making, the subsequent flow-down into the business process and ultimately implementation of the recommended actions at the operations level. These investment decisions are complicated by the fact that techniques and tools for the identification, prioritization and protection of corporate infrastructure are well established. Some findings of note:

- Advancing the capability maturity model to be fully “adaptive” in some cases would not be considered financially responsible, financial goals are driving investment decisions towards bigger risk items.
- Security controls need to be flexible, particularly given the company’s underlying innovation agenda within a dynamic engineering environment.
- Threat and vulnerability information is received from many information sharing forums and sources, it is understood and managed, but automation of indicators is needed.
- Awareness and extension to 3rd parties carry a cost, internal procurement and supply chain policies for major suppliers, small and medium businesses must be considered early on.
- Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from federal, state, and local law enforcement agencies.
- Recovery planning and processes are improved by incorporating lessons learned into future activities.

In a second phase, we explored the application of the Framework to the company’s products and services. This effort was undertaken to answer potential questions from customers as they begin to assimilate products and services into their overall risk management strategy and their application of the Framework. There are several lines of business, communications platforms and their associated infrastructure and subscriber devices that were evaluated. As is industry best practice, MSI continuously monitors products and solutions throughout their lifecycle for adverse security risk based upon the current threat landscape. For example: vulnerability assessments, static code analysis, source code reviews and regulatory compliance are integrated into the development lifecycle. There are also well established techniques and tools— threat analysis and mitigation, secure engineering practices, vulnerability management, software assurance, design process, network and platform security, configuration management, physical security, access controls, application security, incident response and recovery, counterfeit and malware detection, training and awareness.

The one discovery of note during the application of the Framework to products and services was that -- while capable of supporting the Framework methodologies, procedures, and processes -- in most cases these features and functions are the sole responsibility of, and selected by, the end-user. The net of this is that the Framework, as written, requires some reinterpretation and filtering for it to apply to a product and solution development organization. In addition, there is more work to be done around end-user education to enable recommended security features that align policy, business, and technological approaches to address cyber risks; as well as ongoing support to help manage the dynamic nature of the cybersecurity challenge.