LOCKHEED MARTIN

Lockheed Martin Corporation **Original**
RFI– NIST Developing a Framework to Improve Critical Infrastructure Cybersecurity

April 8, 2013

To: The National Institute of Standards and Technology
ATTN: Ms. Diane Honeycutt

Subject: RESPONSE TO RFI DOCUMENT NUMBER: 2013-04413, NIST DEVELOPING A FRAMEWORK TO IMPROVE CRITICAL INFRASTRUCTURE CYBERSECURITY

Dear Ms. Honeycutt,

Lockheed Martin Corporation (LM) is pleased to submit this response to NIST Developing a Framework to Improve Critical Infrastructure Cybersecurity; RFI Document Number: 2013-04413.

LM is a global security company with customers around the world and partners in more than 75 countries outside the United States. Lockheed Martin's 70,000 scientists, engineers, and IT professionals bring a passion for invention as well as significant experience in Cybersecurity systems, products, and services. We are a company that values ethics, integrity, and teamwork in pursuing exceptional performance in our business activities and in ultimately meeting our contractual obligations. LM upholds and demands the highest standards in personal and professional conduct at every level of our business activities.

LM appreciates the opportunity to provide a response to this request for information. Our response includes our perspectives from defending our own enterprise as the largest Defense contractor, our experience working throughout the Government and our work with the commercial critical infrastructure industries. Should NIST require additional information, please refer to the Point of Contact below.

Very respectfully,

William F. Lawrence, Ph.D.
Chief Technology Officer, Cyber Security Solutions
2277 Research Blvd
Rockville, MD 20850
Phone: 301/775-6732
Facsimile : 301/519-6333
Email: william.f.lawrence@lmco.com

Table of Contents

1.0 INTRODUCTION

Lockheed Martin Background Information

Headquartered in Bethesda, MD, Lockheed Martin (LM) is a global security company that employs 120,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services. LM engineers literally span the globe, overseeing more than 4,000 programs at 600 locations in all 50 states and in 75 countries. LM is organized around its core business areas; Information Systems & Global Solutions, Aeronautics, Missiles and Fire Control, Mission Systems and Training, and Space Systems. The corporation has been publicly traded on the New York Stock Exchange under the ticker symbol LMT for over 17 years and reported 2011 sales of $47.2 billion.

As industries continue to evolve at an unprecedented rate, LM is helping them protect the critical infrastructure, networks and systems that power our daily lives. As a global security company, we offer the Cybersecurity expertise that allows us to integrate and protect complex systems. We are helping industries around the world integrate Cybersecurity, improve efficiency and implement information security projects. We apply this expertise across a range of industries including financial services, energy and utilities, pharmaceuticals and manufacturing. ***Security is at the core of all we do.***

LM is the largest information technology provider to the United States Federal Government. We have a rich legacy of integrating and optimizing complex, mission critical information systems in the face of some of the most demanding operational environments. Our technical expertise, operational insights, and systems integration experience gained designing and fielding complex systems provide tremendous value in helping our clients defend their own networks and manage risk.

Lockheed Martin Commitment to Security Innovation

LM makes significant investments in network security to ensure our leadership position. Our approach is to centralize in areas such as providing training, standardizing best practices and offering expertise, while continuing to innovate. Strategic partnerships have been established with companies such as CISCO, Dell, HP, Microsoft, and EMC/RSA. LM's integration strengths, and command and control situational awareness expertise provides adaptive, end-to-end system defense-in-depth capabilities with near real-time detection and response management. LM's participation in the Cyber Security Alliance enhances critical knowledge sharing activities between leading Cybersecurity experts and increases our analysts' technical acumen with various platforms, systems, and software.

Cyber Security Alliance

The Lockheed Martin Cyber Security Alliance combines the strength and expertise of market leading security companies, domain knowledge, and integration into a unique environment called the NexGen Cyber Innovation and Technology Center. Members collaborate on solutions that provide early threat detection, protection, and multi-layer self-healing capabilities to solve customers' hard problems and meet future challenges. These technology partners are engaged in customer-focused solutions, experiments, and systems integration pilots. Alliance companies include: APC by Schneider Electric, CA Technologies, Cisco, Dell, EMC Corporation and its RSA Security Division, HP, Intel, Juniper Networks, McAfee, Microsoft, NetApp, VMware, and Symantec. An alliance approach to Cybersecurity implements solutions that close the seams between product solutions and adds layers of protection from targeted advanced threats. Lockheed Martin's relationship with world-class partners brings increased confidence for mission assurance.

Lockheed Martin Deep Cyber Security Expertise

LM has a 30-year history of developing leading-edge information technologies and associated security standards. We have extensive experience in the areas of governance, standards, and compliance, and we are a leader in the development and support of emerging cyber and network security standards and best practices. We have several thousand Information Security professionals, including over 2,700 with CISSP or Security+ certifications. LM is one of the original authors of the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) and has been involved in the evolution of the National Institute for Standards and Technology (NIST) 800-series of standard publications. LM is active in the Smart Grid Cyber Security Working Group and the Smart Grid

Interoperability Panel Board of Governors. LM actively works with the Nuclear Regulatory Commission, Department of Energy, Department of Homeland Security and Intelligence Agencies, giving us unique insights into the latest threats and vulnerabilities.

LM's approach to providing security as part of enterprise-wide mission solutions is to deploy security controls, such as access control and encryption. These controls are integrated into system architectures from the beginning in order to protect the system from unauthorized disclosure (confidentiality and privacy), unauthorized modification (integrity), and loss of mission availability (resilience and robustness). With secure networks, data fidelity and protection, we help customers eliminate the forces threatening the stability and security of their enterprises.

Lockheed Martin Cyber Security Products and Services

LM continues to develop and deploy innovative capabilities to address threats that are growing in number and sophistication by filling the gaps, challenges, and seams we now face to combat the onslaught of global Cybersecurity attacks. Because of the customers we serve, the sensitive intellectual property we develop, and our role as the largest global security company, LM faces no shortage of threats intent to target us and steal our information. The capabilities we have developed are proven and effective in this complex and dynamic threat environment. The skill sets, methodology, process, and technology we develop for Cybersecurity reflect our keen understanding of sophisticated threats as well as our commitment to protecting our networks and data contained therein.

LM's large global network is under constant cyber attack from a myriad of vectors. Uppermost on this list is the class of threats known as APT. No single Commercial off the Shelf (COTS) product provides the flexibility, agility, or advanced detection capabilities to sufficiently address APT intrusions. Part of what makes these threats "advanced" is the highly targeted nature of their activity as well as the planning and preparation employed by attackers. This preparation includes validating that the malware they use is not detected by current anti-virus or vendor Intrusion Detection System and Intrusion Prevention System (IDS/IPS) signatures. Furthermore, these adversaries develop "zero-day" never-before-seen exploits and malware that the vendor community cannot detect. In light of these challenges, LM developed custom tools to detect these intrusions, quickly pivot through mountains of data, and enable analysts to gather necessary intelligence to detect and mitigate future attacks.

Through our work with our Government and commercial customers, we are directly involved in all the DHS Critical Infrastructure Sectors which presently include:

- Chemical
- Communications
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

LM strongly believes that these sectors are vital to our nation's security, economy, and health. Therefore, providing a strong Cybersecurity Framework is vital to all of our National interests. LM stands ready to work with NIST as you move forward in the development of the Critical Infrastructure Cyber Security

Framework over the coming year. The responses provided in this document were gathered from numerous LM organizations across the corporation. This included different vantage points ranging from our own internal Corporate Information Security organization to those organizations serving our Government and commercial critical infrastructure customers. Through our work with our Government and commercial clients, we are directly involved in all of the DHS Critical Infrastructure Sectors. Since much has been studied, written and standardized for Government operations, the focus of these responses is on identifying, assessing and mitigating risk for the private sector.

The remainder of this document provides LM's responses to each of your questions provided in the RFI Document Number: 2013-04413, NIST Developing a Framework to Improve Critical Infrastructure Cybersecurity.

2.0 CURRENT RISK MANAGEMENT PRACTICES		
	RFI Question	**Lockheed Martin Response**
General	**How do you assess risk; identify the current usage of existing Cybersecurity frameworks, standards, and guidelines; and other management practices related to Cybersecurity?**	Internally, risk is assessed thru an enterprise risk-based business management framework with Cybersecurity as a critical element to identify, assess and take steps to mitigate Cybersecurity risk with respect to capabilities and costs - both internally and throughout our supply chain. The approach to Cybersecurity emphasizes a more comprehensive cyber defense & protection framework rather than a singular focus on best Cybersecurity practices, certifications, and compliance anticipating only risk avoidance. We've learned that adherence to minimum standards is unlikely to provide defense against the sophisticated cyber threat. Enterprise cyber policies, standards, best practices, processes and controls undergo constant reviews and tailoring with emphasis on changing threats, technology advancements, and overall trends. For our customer related work, we manage risk through the use of Risk Management Frameworks, such as: ISACA Risk IT Framework, COSO ERM, NIST RMF, ISO 27001 & FIPS 140-2, NIST 800-53, ISO 27001 and the DOE Cybersecurity Capability Maturity Model. The use of such Risk Management Frameworks requires relevant taxonomies. For these, we consult our own Cybersecurity Capabilities Framework and security control taxonomies developed from leveraging the existing works of NIST, ISO, CoBiT, DoD and CNSS. When no specific requirement is stated, we use NIST SP 800-53 as applicable. We also use a custom-built a Cybersecurity Program Assessment Tool (CPAT) to facilitate the execution of Security Risk Assessments (SRAs) for our clients. While our process is based on the latest NIST best practices the tool also includes requirements and guidelines which are selected based on industry, system scope and applicability. The tool allows our Cybersecurity personnel to make quantitative measurements for risks associated with technology implementation. The scoring system used in this process is derived from, with some modifications, the Common Configuration Scoring System (CCSS) found in NISTIR 7502. We assess Privacy risk through Privacy Impact Assessments, Internal Assessments, Internal Audits, Privacy Reference Architecture, and Privacy Incident Response management.
General	**Are these frameworks, stds, guidelines and/or best practices mandated by legal or regulatory requirements and what are the challenges in meeting these requirements?**	Internally, compliance is evaluated with respect to existing laws, regulations, standards and best practices to include but not limited to: alignment with International Organization for Standardization ISO 27001, National Institute of Standards and Technology Special Publication NIST SP 800-53, and Federal Information Processing Standards FIPS 140-2. For our customer related work, the requirements are sometimes identified for the protection of critical infrastructure such as NE RC and FERC for electric utilities while others do not have corresponding regulatory requirements. We find that the standards are only required on some programs. Whether they are required or just used as an implementation of best practices, limited Industrial Control System (ICS) focus is often a significant problem. The NIST SP 800-53 has some adjustments specified for control systems but it would be easier if there was a guideline that was specifically focused on the ICS environment.

Number	**1. What do organizations see as the greatest challenges in improving Cybersecurity practices across critical infrastructure?**	Our experience with our customers has indicated that the greatest challenges are associated with the perceived ambiguity of the regulatory environment. In those environments that do not have specific requirements, there is a desire for a defined set of "best practice" guidelines. Questions arise such as: Do you mandate verification through a law or offer a reward with the demonstrated security capability? In either case who would pay for the program? Could it be funded out of a legislated fee by business type? Some of the more specific challenges include: • Cyber Requirements Pricing/Cost (Strategy, Planning, Implementation, & Operation); • Data Categorization & Overall Criticality; • Proper Assessment Commensurate with Protection Levels; and • Efficient verification and enforcement across all organizations is a hard problem. Also, there are challenges in improving Privacy Practices such as: governance, awareness, training, communication, and implementation (i.e.: privacy by design).
Number	**2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?**	Through our work with our private sector clients, we see the greatest challenge in developing a cross-sector, standards-based Framework for Critical Infrastructure to be cultural (compliance vs. security focused); the balance and tension between applicability across all industries in contrast to specificity to a particular industry. The inclusion of the full spectrum of risks including internal, external, broad based and targeted is an additional challenge. We also see a general lack of experience in the field, specifically in meeting the need for individuals with experience in Cybersecurity efforts associated with both traditional IT infrastructure and Industrial Control Systems (ICS). A big challenge will be the handling of systems at unmanned, remote sites. None of the current standards address this situation is any depth. They generally assume a manned, protected site model that does not apply to many kinds of distributed control systems. Cybersecurity standard development keeping up with the speed at which threats are evolving is another challenge.
Number	**3. Describe your organization's policies and procedures governing risk generally and Cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?**	Internally, policies and procedures are issued to ensure effective control of operations and compliance with customer, management, legal, and regulatory requirements. Corporate Policy statements exist on Risk Management and Information Security. The statements apply to all employees and Business Areas, including all unincorporated divisions and wholly-owned subsidiaries. Statements are approved by the appropriate members of the Corporate Policy Board and are expressions of management philosophy that may contain implementing instructions and delegations of authority. We have established a comprehensive security program, governed through our Corporate Information Protection Manual. Adherence is enforced by a combination of technical controls, user education and training, a significant Information Security staff, and a disciplinary process executed by our Ethics and Compliance office. While the details of our security practices are highly sensitive, details can be provided on request. Our defense in depth includes: company-wide corporate policies including an information protection manual, division-focused security requirements and procedures, and individual program focused security requirements worked out with our clients. All updates to these documents are advertised to all impacted organizations. Corporate policies also exist that govern the protection of all unclassified corporate assets. These policies are applicable to all businesses & employees and are communicated, supported, and enforced at the local level by business area professionals. Program requirements are dictated per contract specifications and are governed by the respective program security personnel.

		Metrics about the threats targeted at our corporation and the effectiveness of our security controls are communicated on a regular basis to our senior executives and our Board of Directors. Our privacy policies follow the corporation Command Media process and controls. Privacy procedures are documented through Policies, Standard Operating Instructions, or Guidelines. Policies are communicated through corporate communications.
Number	**4. Where do organizations locate their Cybersecurity risk management program/office?**	Internally, our Chief Risk Officer manages the enterprise risk management process and addresses standard and emerging risks from both the Integrated Risk Council and the Risk and Compliance Committee. The committee includes representation from Corporate Information Security. The Chief Privacy Office is located within Corporate Legal. For our clients, the risk management offices vary widely but are often located at the corporate and business area level. Their Cybersecurity risk management program office locations vary. Most frequently we find the Cybersecurity risk management program office in the general Security Office, the Compliance Office, the CIO, or within HR. At the program level the risks are all managed at the program management level and discussed at periodic program management meetings.
Number	**5. How do organizations define and assess risk generally and Cybersecurity risk specifically?**	Internally, the Chief Risk Officer manages the enterprise risk process which includes risk identification, treatment, reporting, and monitoring with the Cybersecurity Risk Model as an element. Our Critical Incident Response Team (CIRT), as well as Corporate Security Enablement, and Security Information Centers are used to monitor, track, and define Cybersecurity Risk and Maturity models. Through our client partnerships, we have extensive experience assessing systems based upon industry best practices and government standards. Our approach when conducting Cybersecurity reviews is to adopt, where appropriate, emerging security requirements from industry best practices, industry groups such as the National Institute for Standards and Technology (NIST), International Organization for Standardization (ISO), the Institute of Electrical and Electronics Engineers (IEEE), and industry specific standards and guidelines, as well as the guidelines being established by regulators and other federal agencies. Cybersecurity risk is part of the overall IT security risk. Security risks are managed in the same integrated discipline as all other program risks.
Number	**6. To what extent is Cybersecurity risk incorporated into organizations' overarching enterprise risk management?**	Internally, the Framework overlays Strategic, Operational, Financial, and Reputational segments. Cybersecurity is an element within the Operational segment. Our Critical Incident Response Team (CIRT), Corporate Security Enablement, and Security Information Centers are used to monitor, track, and define Cybersecurity Risk and Maturity models. They are tightly tied together. All risk to commercial programs are analyzed similarly. Security risks are heavily integrated with safety risks, performance risks, etc. Privacy Risk is incorporated into an Enterprise Risk "Heatmap."
Number	**7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels**	Both internally and for our client engagements, methods vary by priority, plans, reviews, audits, assessments, and updates applicable to the Framework. To understand, measure, and manage privacy risk, we utilize: • Generally Accepted Privacy Principles (GAPP) • Privacy by Design (PbD) • International Organization for Standardization (ISO) • APEC Privacy Framework • U.S. government, Federal Trade Commission (FTC) • Recommendations for Business and Policy Makers • Organization for Economic Co-operation and Development (OECD) Privacy Guidelines • International Association of Privacy Professionals certifications • Guidelines from various state regulators • Industry Association standards and guidelines

		We find that risk assessment is an integral component of the process described in NIST SP 800-39, Managing Risk from Information Systems, An Organizational Perspective. The Risk Management Framework (RMF) described in SP 800-39 provides a baseline for the development of appropriate risk mitigation actions. The RMF includes a well-defined set of information security standards and guidelines that, when implemented, can be used to demonstrate compliance with industry "best practices" for security. We also use NIST 800-53 Rev 3. We also consider Resiliency and Resiliency Management to be important in the continued operations in the face of attack or disaster through a program called "Business Resiliency." Internally focused, the goal of Business Resiliency is to improve LM's ability to withstand significant business disruptions, either due to natural disasters or other large incidents. We focus on the disciplines of Business Continuity, IT Disaster Recovery, Crisis Management and Medical Response (previously, Pandemic Planning). We use the Resiliency Management Model (RMM) to evaluate and help guide us in the development of our corporate command media in these subject areas. RMM does not prescribe specific actions for an organization to take to become more secure. Instead as its title implies, it focuses on understanding what is important to the business and taking a risk-based approach to maintaining a solid protective posture. Internally, we have many common Critical Matrix definitions for employees, partners, contractors, government users and foreign nationals. These include; Smart card/2 factor authentication and dynamic authorization when access behavior deviates from normal on a per user analysis; Security Information Command centers for monitoring/tracking and defining risk posture of external threats; and Cybersecurity Supply Chain Risk Visibility/Assessment Ratings.
Number	**8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to Cybersecurity?**	There are numerous state and federal regulatory requirements relating to Privacy that we follow. Privacy is regulated in the U.S. by the Privacy Act of 1974, and numerous state laws. Certain privacy rights have been established in the United States via legislation such as the Children's Online Privacy Protection Act (COPPA), the Gramm–Leach–Bliley Act (GLB), and the Health Insurance Portability and Accountability Act (HIPAA). Additional Cybersecurity reporting requirements include the annual system Authorization against NIST SP 800-53 and internal audit compliance against corporate/local business unit policy. Currently Cybersecurity events are reported through security incident reporting channels and the annual System Authorization review against the NIST SP 800-53 controls. Also we conduct Internal audits against the Corporate Information Protection Manual (CIPM). Many of our private sector clients have various reporting requirements. For example, our electric utility customers are required to report Cybersecurity status and incidents through the NERC/CIP standards.
Number	**9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?**	This varies widely with each organization. The definition of an "organizational critical asset" is often dependent upon the decisions of each operational environment unless otherwise defined by law, regulation, or generally accepted industry practices.

Number	**10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing Cybersecurity risk?**	Internally, goals vary as a result of a Corporate Information Security Planning Cycle that iteratively updates an executable strategy for mitigating risk of data exposure. Risk mitigation tactical solutions are applied where technically feasible, with approved compliance exceptions required for deviation of policy and threshold specifications. Areas include, for example: • Attrition, risk mitigation, reduction of surface threat and line of business coordination with corporate policy; • Waivers or variances used to define the risk, with each process having its own workflow approval procedures from the line of business that go up to Corporate Information Security; • DR/BCP independent functional directorate and Line of Business (LOB) teams; and • SOX; real-time monitoring and packet capture at the Enterprise Level. We do find, however, that very little consideration for specific "performance goals" related to Cybersecurity are evident with the majority of our customers beyond legal and regulatory compliance.
Number	**11. If your organization is required to report to more than one regulatory body, what information does your organization report and what has been your organization's reporting experience?**	For LM, reporting is voluntary. Our customer Programs/Projects need to meet both the corporate guidelines as well as meeting the Regulatory bodies that are applicable to the specific program customer. There are periodic evaluations against both baselines. In cases where the applicable guidelines differ, the more stringent guideline must be followed.
Number	**12. What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure Cybersecurity conformity assessment?**	Conformity assessments should be a low level priority in the overall objective of protection and situational awareness. Emphasis and practice should include security intelligence as an alternative and more cost efficient option to Cybersecurity risk assessment, certification, and compliance. There needs to be a common or at least harmonized standard, a standardized certification process, and a means of motivating entities to become certified. This may differ in details for different industries, making a common standard challenging. The common standard needs to address the necessary differences while still driving a common mode of operation. There should be a standard governing body overseeing the development and Cybersecurity framework and requirements. National and International standards should be compatible, to the extent practicable, so that a U.S. based global organization can apply a common practice where beneficial and limit compliance activities that may otherwise take resources away from other security efforts. There is some evidence among our clients of a desire for more specific guidance. However, there is also a fear that guidelines could easily become "requirements" that would carry penalties for failure to comply.

3.0 USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES		
	RFI Question	**Lockheed Martin Response**
General	**Provide applicability of existing publications to address Cybersecurity needs, including but not limited to the documents developed by international standards organizations, U.S. Government Agencies and organizations; State regulators or Public Utility Commissions, Industry and industry associations; other Governments and non-profits and other non-government organizations.**	Internally, we developed our own Cybersecurity (CS) Capabilities Framework (Framework) to provide a common set of Cybersecurity terminology as well as a strategic organizing structure. Our Framework is used as a unifying construct for action to reveal strengths and weaknesses in Cybersecurity capabilities. Strategic use of this Framework includes evaluating capabilities of our corporate partners, internal technologies solutions, business units, talent management, and architectural design re-use. Our Cybersecurity Capabilities Framework is not mandated by legal or regulatory requirements. To understand, measure, and manage privacy risk, we utilize: • Generally Accepted Privacy Principles (GAPP) • Privacy by Design (PbD) • International Organization for Standardization (ISO) • APEC Privacy Framework • U.S. government, Federal Trade Commission (FTC) Recommendations for Business and Policy Makers • Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines • International Association of Privacy Professionals certifications • Additional publications and standards applied include SANS Top 20 Controls, NIST SP 800-53 and ISO 27001, DCID, DIACAP, DITSCAP, NERC, FEMA C&A, DoD 8570.1, ITIL, and various SSAAs where applicable. We also support a vast array of customers and programs, each with unique requirements and constraints. In any given program environment there may be one or more frameworks applied, including ISO 17779, ISO 27001, NIST 800-53, DoD Instruction 8500.2, or DISA STIGs. At the corporate level we provide as much flexibility as possible, while still creating an environment that applies appropriate controls. To that end we created a Corporate Information Protection Manual (CIPM) based on controls from several of the major frameworks. ISO 27001 in particular has been fully mapped to our CIPM, and we have attained ISO 27001 certification. For the programs that are contained in a facility the current standards documents like the NIST SP 800-53 and the ISO 27001 are applicable and fairly comprehensive.

General	**Supply information on the current usage of these existing approaches, the robustness and applicability of these frameworks and standards and what would encourage their increased usage?**	Internally, our Cybersecurity Capabilities Framework content provides a taxonomy that rationalizes the wide variety of Cybersecurity activities and capabilities that currently exist or will exist in the future. The CS Capabilities Framework web site itself is constructed as a set of linked wiki pages. This flexible structure allows the community to continually evolve and update its contents to reflect the latest attacks, technologies, standards, and recommended practices. As a result, input to the CS Capabilities Framework web site and its corresponding Reference Libraries is allowed and encouraged by all LM employees. Updates to the site are reviewed by a governance board. The governance board reviews any additions and modifications for suitability. The Framework categorizes Cybersecurity capabilities into a set of Activities. These activities are: Assessment, Engineering, Prevention, Detection, Response & Recovery, Information Operations, and Attack & Exploitation. We created our Corporate Information Protection Manual (CIPM based on controls from several of the major frameworks. ISO 27001 in particular has been fully mapped to our CIPM. We use our experience with the various frameworks to support our customers. Our clients may benefit from a framework that is inclusive of IT and SCADA/control system environments that offers specific guidance for Cybersecurity program development and implementation. Certification and accreditation is a common request from commercial industries looking for a 'seal of approval" for their security programs. Consumers may be drawn to deal with companies that meet a security certification level.
Number	**1. What additional approaches already exist?**	Practices are well known and observed across Critical Infrastructure & Industry as key Cybersecurity risk management components. However, applicability, implementation, and operation are overall business risk decisions. For privacy, we often find that European Union Data Protection Directives and Australian Data Directives apply.
Number	**2. Which of these approaches apply across sectors?**	European Union Data Protection Directives, Australian Data Directives etc. apply against Privacy.
Number	**3. Which organizations use these approaches?**	Depending upon the risk based framework - all, select, few, none, or additional practices (controls, design, operational processes, etc.) may be critical.
Number	**4. What, if any, are the limitations of using such approaches?**	Cost to implement, maintain & monitor, as well as employee skill development & availability, and evolving & sometimes unclear regulation impact activities that can limit profit/sustainability and slow down technological innovation. These efforts along with down-flow impact activities can limit profit/sustainability and slow down innovation. The approaches must ensure the flexibility across multiple industries, allow for evolving threats and technologies, and still be specific enough to result in the intended effects.
Number	**5. What, if any, modifications could make these approaches more useful?**	Modifications to make these approaches more useful are dependent on environment as to threat, design, and operation/business risk assessment. There may need to be a top level framework and then the inclusion of sector specific needs as an integrated model.
Number	**6. How do these approaches take into account sector-specific needs?**	In general, not very well. However, we can say that our Cybersecurity related standards are aligned within the Cybersecurity Risk Model.

Number	**7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?**	Yes, there should be a related sector related, specific standards development process. All frameworks should be tailored to their specific industry. Internally, we have Corporate Policy and associated allocations for internal IT standards that include external alignment, monitoring, and comment. On the other hand, invasive oversight of non-business essential areas may detract from defining the overall risk, threat, and vulnerability of Core and Critical data, processes; information needed to build a strong secure business. This industry tailored approach will encourage participation. It will be necessary to get good buy-in and participation. The framework should offer as much detail as possible on the intent of the guideline and allows for various techniques in which the intent could be met. All frameworks should be tailored to their specific industry. We suggest tailoring the standards/requirements to the specific industry and allow the governing bodies to apply a weighted unbiased rating system across the community. This in turn would make the certification more valuable to the specific sector.
Number	**8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?**	In general, sector-specific agencies and coordinating councils can help to include the sector specific efforts that already exist and continue to evolve as well as ensure participation of sector stakeholders. Agencies can establish and host sector-specific events that promote Cybersecurity efforts and techniques that are specific to that sector. The developed approaches can be published in standard trade publications and presented at sector specific seminars and conferences. Recognition can be given to those entities that demonstrate a high level of "compliance" with the approaches. An example would be to provide different standards/requirements for multiple company categories based on size, product/data/information sensitivity, etc. which would allow sector coordination with governing bodies to apply a weighted rating system that would not be biased across the business community; This rating standard could provide a federated compliance approach allowing companies to assume the same level of Cybersecurity risk when doing business.
Number	**9. What other outreach efforts would be helpful?**	Within sensitive commercial or public infrastructure, a Cybersecurity Simulation standard(s), to include governing bodies with real-time sharing of Cyber intelligence would encourage Cyber Simulation labs for testing and possibly create new business/competition models which would only benefit the evolution and maturity of Cybersecurity frameworks.

4.0 SPECIFIC INDUSTRY PRACTICES COMMENTS		
	Question	**Lockheed Martin Response**
General	**Identify the core practices that are broadly applicable within your organization.**	Internally, all practices are included at varied levels based on resultant risk controls and mitigations from the Enterprise Risk Framework. However, in addition to business policy and specific customer contract requirement/guidance, we employ ISO 27001 requirements and implementation guidelines to assess key policies and supporting activities in the areas of: • Security policy • Organizing information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance • Information security incident management • Business continuity management • Compliance This forms the basis for the LM Information Security Management System (ISMS). We also use our Corporate Information Protection Manual (CIPM) and customer specific guidance.
General	**Supply information on the adoption of the following practices as they pertain to the critical infrastructure components below:** **i. Separation of business from operational systems** **ii. Use of encryption and key management** **iii. Identification and authorization of users accessing systems** **iv. Asset identification and management** **v. Monitoring and incident detection tools and capabilities** **vi. Incident handling policies and procedures** **vii. Mission/system resiliency practices** **viii. Security engineering practices** **ix. Privacy and civil liberties protection**	Our commercial clients are widely familiar with the practices identified in i. – ix. Most have implemented these controls and best practices. However, many have inconsistent or incomplete implementations across their full enterprises. We often encounter systems that do not follow the policies and procedures as defined or where exceptions exist that are not documented. These inconsistencies result in unknown vulnerabilities to the system owners yielding unexpected risk to the business.

Number	**1. Are these practices widely used throughout critical infrastructure and industry?**	We find that with our customer organizations, these practices are well known and observed across Critical Infrastructure & Industry as key Cybersecurity risk management components. However, applicability, implementation, and operation tend to be an overall business risk decision.
Number	**2. How do these practices relate to existing international standards and practices?**	Practices i. Thru viii. can be associated with existing ISOs. These standards generally map well to ISO 27001.
Number	**3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?**	Depending on the risk based framework - all, select few, none, or additional practices (controls, design, operational processes, etc) may be critical. However they cannot be accessed thru text and lists alone. Internally, our core Corporate Information Security controls for our business areas support the research, design, development, manufacture, integration, deployment, fabrication, and operational support of systems and solutions for our customers. Our Information Security Management System comprises frameworks to consistently design, implement, manage, maintain, and enforce Information Security processes and controls and to protect confidentiality, integrity, and availability of information. We leverage the ISO 27001 certification to enhance and create proactive Cybersecurity solutions within our own Cyber Innovation and Technology Center. The most common practices are those dealing with user identification/authorization, physical security, and access control.
Number	**4. Are some of these practices not applicable for business or mission needs within particular sectors?**	All of these practices are applicable to both our internal business and customer mission or business needs. The implementation varies depending on the risk based management framework that is based on business, mission, program, sector, etc. Privacy practices are usually implemented in response to regulatory requirements. Where practices are implemented at an enterprise level, specific implementations need to allow wide variability across a range of systems as often times a single solution or approach is not feasible.
Number	**5. Which of these practices pose the most significant implementation challenge?**	The biggest challenge depends upon the environment as to threat, design, and operational business risk assessment required and result may be a combination. Ongoing challenges are: • Follow up audit reviews to confirm compliance • Address issues in the risk treatment plan • Maintain LM security policy alignment and traceability • Continuous monitoring • CMMI continuous process improvement • Security Intelligence Embedded system and operational systems often pose a significant challenge by the nature of their distributed remote operations, often lower processing and storage capabilities and unique requirements. This creates diversity in the implementation as compared to enterprise data center based IT systems.
Number	**6. How are standards or guidelines utilized by organizations in the implementation of these practices?**	Cybersecurity related Standards are aligned within our Cybersecurity Risk Model. Our Information Security Management System (ISMS) ensures that IS policies and procedures across our Corporation, Business areas, Product lines, Functional organizations, and Programs are aligned, comprehensive, and provide a base for current and future Cybersecurity products and services. The ISMS requirement to continually review and improve our policies and procedures gives our customers confidence in our commitment to best practices, consistency, currency, and agility. Our approach also provides a competitive advantage and reduction in costs connected with improved process efficiency and management of IS costs.

Number	**7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?**	Internally, Corporate Policy and associated allocations exist for internal IT standards that may include external alignment, monitoring, and comment. Our Information Security Management System (ISMS) requires top management engagement in all our organization and product lines across all IS elements. Our corporation benefits from the engagement and visibility of our top management by ensuring that our corporation and customers receive information solutions that maintain confidentiality, integrity, and availability. The ISMS requires that we provide IS corporate governance. We resource corporate information assurance (IA) initiatives, allocate personnel, align technology partners, and task supporting organizations. Our corporate management places a high priority on IS, demonstrating our commitment to current and future customers. However, it is not our experience that this is evidenced across all of our customers. There is wide variability in the maturity and comprehensiveness between industries as well as between different c0ompanies within the same industry.
Number	**8. Do organizations have a formal escalation process to address Cybersecurity risks that suddenly increase in severity?**	Yes, internally we have a formal escalation process that leverages both local and corporate notification paths as severity and situational awareness dictates. Our own Risk and Compliance Committee includes representation from Corporate Information Security supported with a Cybersecurity risk reporting model/process, Cybersecurity Incident Response Playbook and the Privacy Incident Response Playbook. Most, but not all, of our clients have formal escalation processes as well. They vary widely in their completeness and in the communications and awareness to their employees often resulting in policies and processes that exist in documentation but which may not be understood and useful in times of need.
Number	**9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?**	Internally, our Legal organization establishes the detailed requirements for implementing banner statements and disclaimer statements on computing and information systems and related information resources to inform our employees of the security monitoring of our system. Additionally our users and system designers, developers and operators are trained in the impacts to privacy and civil liberties. For sensitive systems additional controls on data security, access and use are provided and additional training and communications are established.

Number	**10. What are the international implications of this Framework on your global business or in policymaking in other countries?**	U.S. and non-U.S. business entities present complex variables by each country for a US Based Company with International Locations. The majority of our work is for the US government, so we concentrate on NIST SP 800-53 and ISO 27001. They agree in most areas although there are exceptions. We make every effort to have ISO involved in any planned infrastructure work so that we have compatible international standards. The privacy laws in some countries do impact system design, operations and controls and may require data segregation as well as additional limitations on data access and usage. Our Information Security Management System (ISMS) encourages global problem-solving across all aspects of information security including our people, processes, teammates, and partners as well as our hardware, software, and networks suppliers. ISMS requirements ensure that our total organization works together to ensure IS in our deliverables including our: • Engineering and technology organizations • Performance and operating excellence organizations • Enterprise Business Solutions (EBS) and Chief Information • Office (CIO) organizations • Global supply chain management organizations • Human resources and Talent and Organizational Development (T&OD) organizations • Finance and business organizations • Security operations and continuity of operations organizations. International implications are based on regional government regulations which need to account for the regional variations in regulation.
Number	**11. How should any risks to privacy and civil liberties be managed?**	In accordance with existing policy and regulatory guidance. This should be handled like Personally Identifiable Information with no access to non-anonymous data. Privacy risks should be mitigated and minimized through governance, awareness, training, communication, and implementation (i.e: privacy by design, and no access to non-anonymous data).
Number	**12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?**	Yes the Framework should include risk methodology based practices as required based on the business analysis and assessment. Other areas to include are: • Commitment to Training • Enhancing Knowledge, Skills, Abilities; and Employee Awareness Internally, our Information Security Management System (ISMS) requires an organizational commitment to awareness and training that delivers direct benefits to our current and future customers and our corporation. We apply a rigorous talent management initiative containing a complete career path and compensation component to identify Information Security or Information Assurance experts in designing and implementing total life cycle production and servicing solutions. We continually work to obtain leading expertise via our experienced professional acquisition activities as well as our college recruiting and STEM outreach activities. In 2008, we introduced a Cyber University to ensure our Cybersecurity subject matter experts (SMEs) receive and maintain leading edge training and access to courses that enable them to attain relevant Cybersecurity accreditations. We also require comprehensive yearly awareness training for every employee as well as provide ongoing communications about emerging threats changes to our policies, procedures and technical controls to mitigate these risks.

5.0 ISA FRAMEWORK SURVEY

Additional response requested on the practices below. This data will be used to help guide the NIST RFI collection in addition to serving as LM input to ISAlliance. The ISAlliance promotes sound security practices. The survey responses will reflect what good security companies should be doing and may aid in illustrating what a practical baseline framework might look like. Results will be presented in aggregate form without specific company identification.

Proven Effective Cybersecurity Controls	Lockheed Martin Status	Lockheed Martin Comments
Cross-departmental Executive vested with strategic control of cyber systems.	Currently implemented	
Establish a cross-enterprise "Cyber Risk Team" to identify cyber risk.	Currently implemented	
Have regular "Cyber Risk Team" meetings.	Currently implemented	
Develop and adopt a cyber risk management plan.	Currently implemented	
Develop and adopt an enterprise cyber risk budget.	Currently implemented	Not just a "risk" budget, but a full Cybersecurity program management budget.
Implement, Analyze, Test, and Feedback	Currently implemented	
Eliminate unnecessary data and inventory and monitor what is left.	Currently implemented	Consideration for the importance and sensitivity of all data should be given.
Ensure essential controls are met; regularly audit to make sure these controls remain met.	Currently implemented	Yes, but also audit the actual effectiveness of the control. It is important to note that just because a control is in place does not necessarily mean that it is effective.
Change default credentials / administrative passwords.	Currently implemented	
Avoid shared credentials.	Currently implemented	
Implement a firewall or access control list (ACL) on remote access/administration services.	Currently implemented	
Update Anti-Virus and Other Software.	Currently implemented	
Utilize IP "Blacklisting."	Currently implemented	
Audit User Accounts.	Currently implemented	
Restrict and monitor privileged users.	Currently implemented	
Monitor and filter outbound network traffic.	Currently implemented	
Proven Effective Cybersecurity Controls	**Comments**	**Comments**
Application testing and code review.	Currently implemented	A component of a comprehensive secure system development lifecycle methodology.

Monitor and mine event logs.	Currently implemented	Yes, but also develop methodologies for the review and assessment of the information in the logs. Also develop and implement appropriate actions to information discovered during audit log reviews.
Change monitoring and log analysis approach to one that is pragmatic and can be implemented.	Currently implemented	
Define "suspicious" and "anomalous" and then monitor for it.	Currently implemented	Yes. But the definitions could prove to be limiting and the implementation of detections of anomalies and suspicious behaviors needs to be dynamic to keep pace with emerging and changing threats.
Train employees to be aware of social engineering methods.	Currently implemented	
Train employees/customers to look for signs of tampering and fraud.	Currently implemented	
Create an Incident Response Plan.	Currently implemented	
Engage in mock incident testing.	Currently implemented	
Assess Vendors for Security.	Currently implemented	
"Whitelist" Applications.	Currently implemented	
Application Patching.	Currently implemented	
Patch Operating System(s).	Currently implemented	
Minimize "Administrative Privileges."	Currently implemented	
Utilize "Continuous Monitoring."	Currently implemented	This must be based on the operational environment. Should not be a "blanket" requirement.