Honeywell

Developing a Framework to Improve Critical Infrastructure Cybersecurity

Request for Information

Docket Number 130208119-3119-01

NOApril 8, 2013

Submitted to:
National Institute of Standards and Technology
ATTN: Diane Honeycutt
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

Submitted by:
Honeywell Technology Solutions Inc.
7000 Columbia Gateway Drive
P.O. Box 5555
Columbia, MD 21046-5555
Phone: 410-964-7000
Fax: 410-964-7300
www.Honeywell.com/HTSI

TABLE OF CONTENTS

Section **Page**

TABLE OF CONTENTS (Continued)

Section **Page**

EXECUTIVE SUMMARY

Honeywell is pleased to respond to the National Institute of Standards and Technology's (NIST) request for information regarding "Developing a Framework to Improve Critical Infrastructure Cybersecurity." We are well positioned as a supplier of critical infrastructure products and services to offer valuable insight into the NIST request. This executive summary describes our company's multiple positions in the critical infrastructure supply chain and our approach to this response.

Honeywell believes that the framework should be risk-based and capable of keeping pace with evolving threats. It should advocate and not mandate good security practices and be a component of a predictive cyber security process that is supplemented with effective information sharing between government and industry partners. We welcome the recent Presidential Executive Order and also believe the Federal agencies must commit to share information, including classified information, in real time.

Our responses contain the perspectives of several Honeywell cybersecurity stakeholders:

- A supplier of critical infrastructure products and services to public and private sectors
- A customer partner within the Department of Defense (DoD), Aerospace and Energy markets
- An enterprise security group that manages our enterprise security program
- An industry expert on critical infrastructure processes in transportation and energy sectors.

Honeywell is a Fortune 100 company that invents and manufactures technologies to address tough challenges linked to global macro-trends such as safety, security, and energy. With approximately 132,000 employees worldwide, including more than 22,000 engineers and technologists, we have an unrelenting focus on quality, delivery, value, and technology in everything we make and do. With 97 distinct research and engineering facilities, we have over 32,000 patents and patents pending. Our businesses deliver products and services supporting critical infrastructure primarily in the spaces of Industrial Energy and Aerospace Transportation. Further, we provide on-going Security Solutions for both our internal enterprise and our external customer base.

Industrial Energy - Honeywell Automation Controls Solutions is a leader in Industrial IT Solutions focusing on protecting process industry facilities from the growing risk of industrial cybersecurity threats and vulnerabilities. The portfolio includes scalable tools, services, best practices, and support from Honeywell's global team of network- and security-certified personnel that secure users' critical infrastructure and deliver a more predictable and safe environment – regardless of control system vendor or location. Honeywell draws on its experience in more than 70 control system versions and hundreds of key industrial cybersecurity projects across the globe to provide a bottom-up, asset-based security risk management solutions that are customized to process control environments. We are at work in 150 million homes, 10 million buildings, 5,000 industrial facilities, and hundreds of gas and electric utilities worldwide.

Aerospace Transportation - Honeywell Aerospace is a leader in developing and certifying new safe and secure products to connect aircraft to external network-oriented services. We innovate and integrate thousands of products and services to advance and easily deliver safe, efficient, productive, and comfortable experiences worldwide. Our goal is to secure these aerospace products and services by adding cybersecurity concerns and certifications to our existing risk

management practices for development and operation, including the development of new and novel cybersecurity technologies for achieving these goals, and diligence in analysis and response to developing cybersecurity threats to our products and services.

Enterprise Security Solutions - Honeywell Global Security is our internal security organization that is accountable for the physical and cybersecurity across the Honeywell enterprise. Its portfolio includes: internal policy and standards; business continuity; risk assessments; architecture and our Security Operations Center (SOC) that coordinates threat monitoring and incident response.

External Security Solutions - Honeywell Technology Solutions is the Federal Security Services arm for Honeywell's diverse product lines. We partner with our businesses to deliver physical and cyber solutions to both public and private entities. Key capabilities include policy transition and training, auditing, risk assessment, certification and accreditation, intelligence, site remediation, security deployment and installations and on-going computer network defense.

Our responses leverage this diverse perspective and experience with critical infrastructure protection. Our key themes are:

- A "one size for all" approach is not effective. Critical infrastructure is diverse; the threats and their solutions vary. We recommend tailoring by sector.
- Standards must be risk-based and flexible and capable of keeping pace with evolving threats. They should promote the value of meeting objectives and should not prescribe the means of compliance.
- We do not support standards that require "check the box" assessments and or static control frameworks.
- We encourage NIST to define the relationship of the new framework with other current standards and/or policies already in place.

Our responses are linked to each question in the Request for Information (RFI) and organized by the three RFI topics: Risk Management; Use of Frameworks, Standards, Guidelines, and Best Practices; and Specific Practices. Please do not hesitate to contact us for further clarification.

CURRENT RISK MANAGEMENT PRACTICES

Cybersecurity risks should be regularly evaluated at the leadership and operational levels. Product teams and enterprise security groups should prioritize these risks to improve predictive capabilities and reliability for products and services. Cybersecurity standards should be relevant, risk-based and capable of keeping pace with evolving threats. Each critical infrastructure sector will have varying risk tolerances based on the services they provide. To that end any risk framework should allow flexibility.

WHAT DO ORGANIZATIONS SEE AS THE GREATEST CHALLENGES IN IMPROVING CYBERSECURITY PRACTICES ACROSS CRITICAL INFRASTRUCTURE AND WHAT DO ORGANIZATIONS SEE AS THE GREATEST CHALLENGES IN DEVELOPING CROSS SECTOR STANDARDS BASED FRAMEWORK FOR CRITICAL INFRASTRUCTURE?

The challenges seen can be describe in three areas: technological, sector uniqueness and mission assurance.

Technology Challenges. Layering technology on top of critical infrastructure that was not originally designed for a security layer must be carefully implemented to avoid causing impacts to safety, performance and functionality adding unreasonable cost. Much of the critical infrastructure has a lifetime measured in decades as opposed to the 3-5 year life of typical IT equipment. This legacy equipment was deployed at a time when the threat was low and the cost of computing and communications were high. Much of this legacy equipment cannot be practically upgraded to address these security concerns and thus requires replacement in order to significantly improve security.

Sector Uniqueness Challenges. Controls that provide for flexibility on implementation methodologies can mitigate the challenge of force fitting solutions into differing environments which may cause significant disruption if not tailored. The experience of the Aerospace sector in implementing integrated risk management practices under Federal regulation is that frameworks work best when they focus on the objectives for compliance and not on the means of compliance. Information technology practices vary across sectors and even within sectors in order to satisfy the specific functional needs that drive an organization to adopt information technology. Practices that are standard within one sector may conflict with the technology requirements of another sector and could even conflict with a different segment of the same sector.

Part of sector unique challenges is the management of conflict across standards. Under the auspices of Department of Transportation (DOT), Federal Aviation Authority (FAA), and the International Civil Aviation Organization (ICAO) for example, the Aerospace sector is already subject to a standards-based framework to assure the safety of the public which includes the threats of cybersecurity attack, and has integrated practices and processes to assure compliance with safety regulations and standards. Any cross-sector cybersecurity framework must be compatible with the existing safety practices and processes.

The priority of control implementation within a framework needs to address threats and consequences of cyber attacks against sector specific critical infrastructure. For example, the consequences are much different between disabling an elevator versus disabling an aircraft or power plant thus the control priorities will be different. The range of consequences also

determines the need for varied levels of investment to address cybersecurity across the sectors and applications.

Cybersecurity best practices and controls should be balanced with the threats and unique risk tolerances of each critical infrastructure sector. Existing and overlapping practices need to be consolidated, simplified and supplemented with effective sharing of threat information between government and peer companies.

Mission Assurance Challenges. Many of the control systems for critical infrastructure are complex, distributed and safety critical. Getting systems to function safely and efficiently is already a significant engineering challenge. When additional security measures are layered on top of these systems it can lead to significant changes in operational procedures. For example, locking down security in safety critical systems may require over-ride technology/procedures to be implemented to allow access to controls in the event of an emergency.

Controls must add value in increasing the security posture of critical infrastructure. Paperwork documentation or simply reporting the security state does not make the systems more secure, but rather simply documents the vulnerabilities. The framework must allow public and private concerns to implement the controls at some level, increasing security, without negatively impacting mission requirements.

Consideration must also be given to the criticality of each control based upon the implementation environment. Examples can include specific business-sectors (Finance, Manufacturing, Services, etc.); the framework should allow the ability to identify similar threat vectors between sectors; factor in each group's unique risk tolerances; and design road maps to prioritize security investments around each sectors most critical mission elements. It is not feasible to drive specifics across sectors, but rather more reasonable to identify risks in the form of controls and allow the individual sectors to define the actions that are necessary to secure their products to meet their missions.

DESCRIBE YOUR ORGANIZATIONS POLICIES AND PROCEDURES GOVERNING RISK GENERALLY AND CYBERSECURITY RISK SPECIFICALLY. HOW DOES SENIOR MANAGEMENT COMMUNICATE AND OVERSEE THESE POLICIES AND PROCEDURES?

Senior management considers cybersecurity to be a fundamental part of safety risk management and product certification, and a fundamental process within the development and production of critical infrastructure products. Development, propagation, and enforcement of cybersecurity policies and procedures is part of the Integrated Product Development, Delivery and Service processes used by Honeywell in all development and production. Enforcement of these processes is considered a fundamental Honeywell value by senior management. For our Avionics products, the process is audited by FAA personnel to demonstrate compliance to Federal process standards. For our DoD products and services, Authority to Operate must be granted by the government’s Designated Approval Authority prior to operation. For those customers whom we provide risk assessment services for, we utilized a framework of identification, prioritization and mitigation which is based on a combination of severity, likelihood and ability to mitigate.

Cybersecurity risk is governed at the enterprise level through a Governance Risk and Compliance framework. As an example,

- Risk objectives are defined; critical assets are identified; and tiered controls are established.

- Control owners are appointed and control effectiveness managed by visual management processes.
- Protocols for escalation of control failures are defined; business continuity management plans are implemented and tested.
- Risk is continuously assessed based upon dynamic threat conditions and threat intelligence.
- Leaders periodically audit risk objectives, controls, and plans.

WHERE DO ORGANIZATIONS LOCATE THEIR CYBERSECURITY RISK MANAGEMENT PROGRAM/OFFICE?

All programs and product deployments have a risk program that they follow regardless of the physical location of that activity. In many cases the risk management office is centrally located while others are located at the site of the activity. Each product development program develops and executes a cybersecurity plan conforming to the appropriate governing and compliance body.

The Chief Information Officer is accountable and the Chief Security Officer is responsible for cybersecurity risk management at the enterprise level.

HOW DO ORGANIZATIONS DEFINE AND ASSESS RISK GENERALLY AND CYBERSECURITY RISK SPECIFICALLY?

Generally, risk is managed through a combination of impact, likelihood of occurrence and ability to mitigate. Because these factors for cybersecurity risk can be different across sectors, industry looks to compliance and standard documentation to identify key controls for their sector.

At the enterprise level focus is on risk that has a significant impact on critical assets and services. Key steps include assessing damage potential, determining reproducibility and exploitability, establishing the ability to detect and identifying affected people.

Within the Aerospace Transportation sector, the definition and assessment of risk is typically governed by control sets applicable to the respective area. For example, Federal regulations Code of Federal Regulations (CFR) Title 14 25.1309 and CFR Title 14 25.1301 define acceptable risk compliance for aircraft equipment, which includes the risk from cybersecurity threats. The FAA issues means of compliance to these regulations for failure and operational risk in Advisory Circular (AC)25.1309 which also refers to additional guidance in the industry standards Society of Automotive/Aerospace Engineers (SAE) Aerospace Recommended Practices (ARP) 4754 and SAE ARP 4761. An extended means of compliance for cybersecurity risk assessment is defined in Radio Technical Commission for Aeronautics (RTCA) DO-326 "Airworthiness Security". Other standards also apply based on FAA requirements for specific products. Honeywell conforms to these standards in all its internal development processes.

Programs for critical infrastructure within the DoD follow 8500.1 and 8500.2 controls and compliance analysis utilizing documents such as the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Implementation Plan (DIP), System Implementation plan (SIP), Assessment Scorecard and Plan of Action and Milestones (POA&M) to define and assess cyber security risk. Annual validations of system controls are done to ensure risk is being reduced and the overall security posture of systems is being increased.

In all these sectors, Stakeholder agreement is paramount to risk acceptance. These stakeholders may be governing bodies, Designated Approval Authorities or the company's Senior Management. They must decide which risks should be addressed through the approved mitigation plan or determine which risks should be accepted or transferred.

TO WHAT EXTENT IS CYBERSECURITY RISK INCORPORATED INTO ORGANIZATION OVERARCHING ENTERPRISE RISK MANAGEMENT?

Within the enterprise, cybersecurity risk is initially evaluated at the operational level through recurring audits, risk assessments, incident management and root cause analysis. Findings are reviewed and assessed by appropriate business and corporate teams. Cybersecurity risk is reviewed and evaluated each year for purposes of updating the Audit Committee and in support of certain Securities and Exchange Commission (SEC) requirements, e.g., 10-K disclosure.

For products and service offerings, it is fully incorporated into the Integrated Product Development Process used by our development and manufacturing operations.

WHAT STANDARDS, GUIDELINES, BEST PRACTICES, AND TOOLS ARE ORGANIZATIONS USING TO UNDERSTAND, MEASURE, AND MANAGE RISK AT THE MANAGEMENT, OPERATIONAL, AND TECHNICAL LEVELS?

There is not a single standard that fits across all areas (Site, Organization, and product/program) but rather a set of sector specific guidance. Some of these include:

- International Electrotechnical Commission (IEC) 62443/ISA-99 standard for Industrial Automation & Control Systems Security is used within the process automation industry.
- AC25.1309, SAE ARP 4754, SAE ARP 4754A, SAE ARP 4761, SAE ARP 5150, and DO-326 for Avionics Development. Other regulations and standards apply to airline operators, and the Federal ATC system is subject to FISMA.
- International Organization for Standardization (ISO)/IEC 27000-series, NIST Special Publications -800 series, Control Objectives for Information and Related Technology (COBIT), Information Technology Infrastructure Library (ITIL) for IT organizations.
- DoD best practices including DIACAP, NIST 800-53 and ISO 17000 series.
- Others include Federal Information Security Management Act (FISMA), Federal Information Processing Standard (FIPS), and miscellaneous NIST SPs.

In addition, companies can choose to develop internal policies and standards via industry associations such as the Information Security Forum and Information Risk Executive Council and Network Frontiers (ICFs).

WHAT ARE THE CURRENT REGULATORY REPORTING REQUIREMENTS IN THE UNITED STATES (E.G. LOCAL, STATE, NATIONAL AND OTHER) FOR ORGANIZATIONS RELATING TO CYBERSECURITY?

There are numerous reporting requirements. Some are linked to a mandate for corporate reporting and some are specific to business sectors and product lines.

Product/program reporting requirements are governed by the compliance clauses levied by the regulating authorities such as the FAA issuing Special Conditions under CFR Title 14 for managing the cybersecurity aspects of Type Design, Production Approval, Continuing Airworthiness, and Operational Approval of all aerospace commercial products and services. For

DoD compliant mission systems the reporting requirements include DoD 8500 series documentation (DIACAP) including DIP, SIP, Score card and POA&M artifacts.

WHAT ORGANIZATIONAL CRITICAL ASSETS ARE INTERDEPENDENT UPON OTHER CRITICAL PHYSICAL AND INFORMATION INFRASTRUCTURES, INCLUDING TELECOMMUNICATIONS, ENERGY, FINANCIAL SERVICES, WATER, AND TRANSPORTATION SECTORS?

Our businesses are diverse and are interdependent with many critical infrastructure sectors including financial, telecommunications, transportation, energy, chemical, information technology and manufacturing sectors.

From the perspective of a critical infrastructure product supplier, integration of critical infrastructure into its operational environment will include at a minimum, power, heating and cooling, physical security system, cybersecurity systems, human interface, transportation and telecommunications.

WHAT PERFORMANCE GOALS DO ORGANIZATIONS ADOPT TO ENSURE THEIR ABILITY TO PROVIDE ESSENTIAL SERVICES WHILE MANAGING CYBERSECURITY RISK?

These goals vary by business sector; generally both qualitative and quantitative measurements can be used to define acceptable levels of performance during an emergency; these include incident management response time and the level of preparedness to respond to a cyber crisis based on different scenarios; and also the percentage of continuity of operations plans and procedures that have been tested.

From a product perspective the goals must be commiserate with the environment in which they apply. For example the single most critical performance goal in avionics is to maintain the safety to the travelling public of the air transport system. Continuity of business is the next most important, but is considered secondary to safety. For controls systems, priorities may be given to availability and integrity first and confidentiality second.

IF YOUR ORGANIZATION IS REQUIRED TO REPORT TO MORE THAN ONE REGULATORY BODY, WHAT INFORMATION DOES YOUR ORGANIZATION REPORT AND WHAT HAS BEEN YOUR ORGANIZATIONS REPORTING EXPERIENCE?

A very key point must be made that providing the same report to multiple regulatory bodies causes conflict both within and across sectors. Honeywell recommends a single entity for each individual critical infrastructure Sector. The content of what we report is generally defined within our contract/customer agreements. Our experience of providing cybersecurity information to more than one entity even within the same governmental organization is difficult due to the varying entities wanting different kinds of information used for different purposes. In some situations where there are overlapping responsibilities, agencies are inconsistent with their oversight and with their inter agency communications.

WHAT ROLES(S) DO OR SHOULD NATIONAL/INTERNATIONAL STANDARDS AND ORGANIZATIONS THAT DEVELOP NATIONAL / INTERNATIONAL STANDARDS PLAY IN CRITICAL INFRASTRUCTURE CYBERSECURITY CONFORMITY ASSESSMENT?

Many operators of critical infrastructure operate in more than one country. In addition, vendors providing products and services to critical infrastructure almost always sell their products and

services globally. Therefore, any standards or frameworks adopted in the US must be coordinated with international standards. This allows US vendors to remain competitive in the world market by providing a single product which meets both US and international standards.

Cybersecurity conformity requires clear enumeration of requirements and testing against those requirements. This is challenging in cybersecurity given software and network interdependencies. Before conformity assessment standards are developed for critical infrastructure, organizations should invest in developing guidelines that address these challenges. The guidelines should then be used on a voluntary basis to assess usefulness and then standards rolled out. Although the standards may vary across international boundaries, the intent would be for these organizations to provide the requirements and accepted means of compliance to the requirements for the assessment of designs and operating policies and procedures for critical infrastructure. Examples include avionics products within the National Air Spaces and Controls Systems within the power generation space.

Additionally, partnerships with such groups as the Information Security Forum (ISF) have been beneficial. Specific standards and white-papers have been instrumental in setting Honeywell's cyber resilience strategy. (ISF 2011 Standard of Good Practice for Information Systems Report and ISF Cybersecurity Strategies - Achieving Cyber Resilience Report)

USE OF FRAMEWORKS, STANDARDS, GUIDELINES, AND BEST PRACTICES

There are numerous frameworks, standards and best practices. Most of the published ISO/IEC 27000-series, NIST SP 800-series, COBIT, ITIL and ISF Good Practices apply across sectors. This is an excellent opportunity for NIST to test the effectiveness of standards-based approaches and gain lessons learned. Standards should be rationalized to meet the needs of each sector. They should provide a foundation that can be customized for a diverse set of business models and must be flexible to meet the needs of the business without overburdening the technology. The content should be simple to understand.

WHAT ADDITIONAL APPROACHES ALREADY EXIST

Approaches for frameworks are similar, being comprised primarily of identifying risk, assessing impact of risk, prioritizing the risk and taking action on the risk. Continual assessments of new threats and their impact to the security posture of an asset is also a standard part of a best practices framework.

However, at the standards and guideline levels, diversity occurs across sectors almost immediately since the risk identification, impact and priorities vary. Much of this variance manifests itself in standards and applicable controls. There are numerous regulations and standards already in place. Listed below are a few of those.

- ISA 95 and IEC 62443/ISA 99 standards which are widely respected and increasingly adopted within the process control industry.
- CFR Title 14 regulations on acceptable risk to the public for aerospace products and services. These include Integrated Safety Risk Management, Development Assurance Processes, Safety Assessment of Design, Systems Engineering and Requirements Management. An initial set of high-level standards covering these areas would include FAA AC25.1309, SAE ARP 4754, SAE ARP 4754A, SAE ARP 4761, SAE ARP 5150, RTCA DO-178C, RTCA DO-254, RTCA-DO-278, and RTCA DO-326. Other regulations and standards apply to airline operators, and the Federal Air Traffic Control (ATC) system is subject to FISMA.
- Within the enterprise the use of the Unified Compliance Framework (UCF) is heavily leveraged. The UCF maps ISO/IEC 27000-series, NIST Special Publications -800 series; COBIT, ITIL; ISF standards of good practice, amongst others, such as Federal/state/country agencies and organizations. In addition, relationships with Industry Forums have been used to our advantage, e.g., ISF 2011 Standard of Good Practice for Information Systems Report and ISF Cybersecurity Strategies - Achieving Cyber Resilience Report.
- DIACAP 8500 approach for DoD certification.

WHICH OF THESE APPROACHES APPLY ACROSS SECTORS?

Although, in general, good practices and frameworks should be applicable across sectors, at the control level, they lack the granularity to make the controls set highly useful or lack the implementation/execution elements that will actually increase the security posture vs. just documenting it. This has led to the numerous standards and compliance documents we see today; each with their own set of sector specific controls. The overall implementation of those controls varies widely due to the nature of the performance, functionality and usage requirements of critical infrastructure products. As stated previously, one cannot assume critical infrastructure

controls within an operational environment are directly mapped to Information Technology (IT) controls used within a company's IT environment.

It is however, worthwhile to review the various sector standards currently in place and determine their broadness within a sector. For example:

- ISA standards are used extensively in the oil and gas sectors. These approaches apply to some portions of the electric sector.
- Various FAA standards were written specifically for use by the Aerospace sector to satisfy national and international regulations for safety and security. Most are written generally enough to be applicable to all sectors, but adoption outside Aerospace is extremely limited.

WHICH ORGANIZATIONS USE THESE APPROACHES?

These approaches are widely used across the industry for the products that are supplied into the critical infrastructure sectors for both commercial and federal customers. In most cases compliance must be met in association with the standards that are embedded in the approach.

Enterprise Security groups leverage the UCF while IT is more closely linked to frameworks such as ITIL and COBIT. Key principles associated with these approaches and good practices are integrated into internal policies and standards that are used by operations, compliance groups and Steering Committees.

WHAT IF ANY ARE THE LIMITATIONS OF USING SUCH APPROACHES?

In all cases of a company's central infrastructure, a development program or a site deployment, the approach must be integrated into the basic processes of the organization and must be highly measurable. The standards are in many cases interdependent, so it can be difficult to implement a subset of the standards while ensuring completeness. The division of responsibilities between the different standards reflects the division of responsibilities between organizations in a particular sector which may not be representative of other sectors.

Cost can also play a factor in ensuring an approach has longevity. Some standards must be purchased including updates. This may make consistency across companies even within a sector more difficult. Limitations are based on the willingness to adopt and the expense to comply. Since return on investment is typically not easily quantifiable for security, inconsistencies on the degree of adoption can occur.

Lastly, trying to generalize the controls for broader usage can render them ineffective and less valuable when implemented.

WHAT IF ANY MODIFICATION CAN MAKE THESE APPROACHES USEFUL?

Any common framework must be able to insert appropriate and flexible standards to meet the needs of each sector. It should provide a foundation that can be customized for a diverse set of business models / critical infrastructures and must be flexible to meet the needs of the business without overburdening the technology. The content should be simple to understand.

HOW DO THESE APPROACHES TAKE INTO ACCOUNT SECTOR-SPECIFIC NEEDS?

There are essentially three layers to this approach; the first involves those controls that can span sectors. Elements such as the inclusion of a disaster recovery plan or the implementation of redundancy may fall in this category. The 2nd layer contains those controls within a sector that

might span differing sub-sectors. Lastly, there is a layer of controls that are specific to a sub-sector which are either not applicable or not implementable across multiple sub-sectors, but only apply to a specific sub-sector.

These approaches are based on managing the requirements and implementations of a specific sector. Sector-specific needs and practices are managed naturally by their inclusion in the requirements. Additionally, sector specific agencies develop standards and requirements that can result in overlapping compliance requirements and the cost of this overlap must be factored in to the controls framework. Lastly, the currency of the standards must be considered in order for them to keep up with the pace of the threats for a particular sector.

WHEN USING AN EXISTING FRAMEWORK, SHOULD THERE BE A RELATED SECTOR-SPECIFIC STANDARDS DEVELOPMENT PROCESS OR VOLUNTARY PROGRAM?

Any framework must be tailored to the specific sector. The working members of those sectors must have input. Standard practices vary widely between sectors and even between different roles within a given sector. It would not be feasible to mix sector members. The traditional 'one-size-fits-all' approach is ineffective. Developing a way to group sectors/industries, (example; by threat vectors and or "personas"), provides the opportunity to implement rational solutions capable of enhancing cybersecurity without degrading business operations.

WHAT CAN THE ROLE OF SECTOR-SPECIFIC AGENCIES AND RELATED SECTOR COORDINATING COUNCILS BE IN DEVELOPING AND PROMOTING THE USE OF THESE APPROACHES?

There are several valuable roles that agencies can play including:

- Becoming an active participant in the Defense Industrial Base Sector Coordinating council (DIB SCC).
- Coordinating existing sector agencies, standards organizations, and other interested parties ensuring that conflicting direction is not given to industry suppliers.
- Advocating reasonable and adequate controls and security capabilities that target the specific threats impacting the specific sector/industry.

WHAT OTHER OUTREACH EFFORTS WOULD BE HELPFUL?

In order to measure success in terms of increasing the security posture a standardized, yet non complex process to measure the maturity of an organization's security controls and capabilities against frameworks like ISO and NIST would be helpful. This will enable organizations to identify security gaps and implement and upgrade; thus avoiding over/under security investments. As always, continual communications with industry partners is appreciated.

SPECIFIC INDUSTRY PRACTICES

The use of core security technologies, practices and processes, where not governed by regulation, are typically leveraged in varying degrees to different levels of success. For example, although encryption & key management is leveraged for many systems, it is certainly not leveraged by all and is managed differently depending on the organization's appetite for risk.

ARE THESE PRACTICES WIDELY USED THROUGHOUT CRITICAL INFRASTRUCTURE AND INDUSTRY?

Outside of compliance and regulatory standards required, industry may additionally, utilize best practices within product/program development and manufacturing processed. Included below are routine practices used in the energy sector.

- Separation of business from operational systems
- Mission/system resiliency practices
- Security engineering practices.

Under the auspices of DOT, FAA, and ICAO, the Aerospace sector is already subject to a standards-based framework for risk management practices to assure the safety of the public, a framework which includes the threats of cybersecurity attack. Since commercial air transport was first begun, the sector has integrated practices and processes to assure compliance with these safety regulations and standards. Aerospace risk management controls include versions of all of the cybersecurity framework controls, but are implemented through practices that are both different from, and more rigorous in their enforcement, than the corresponding practices in many other commercial sectors.

Our experience regarding enterprise implementations show that, where not governed by regulation, the use of core security technologies, practices and processes by companies is inconsistent. The inconsistencies are driven in part by differing risk tolerances within lines of business, sector and sub-sector.

HOW DO THESE PRACTICES RELATE TO EXISTING INTERNATIONAL STANDARDS AND PRACTICES?

For product deliveries these practices are generally universal. For example, interoperability, compatibility and reciprocity between national agencies and airspaces have meant that these practices have been or will be largely reflected in existing international standards and practices.

Many companies also align with international standards such as ISO.

WHICH OF THESE PRACTICES DO COMMENTERS SEE AS BEING THE MOST CRITICAL FOR THE SECURE OPERATIONS OF CRITICAL INFRASTRUCTURE?

Sector priorities will differ. Honeywell provides guidance below for the energy sector and the aviation portion of the Transportation sector as well as enterprise guidance. Energy practice high priorities:

- Separation of business from operational systems
- Use of encryption and key management
- Identification and authorization of users accessing systems

- Security engineering practices
- Mission/system resiliency practices
- Monitoring and incident detection tools and capabilities
- Incident handling policies and procedures
- Asset identification and management
- Privacy and civil liberties protection.

That said, the priority and adherence of these practices is determined by a range of factors and flexibility is prudent to assure broad adoption.

Aviation practices themselves are not critical. What is critical is the means to evaluate the effectiveness and completeness of a proposed set of controls. Key concerns include safety and reliability (continuity of business).

Within the confines of internal company operations, mission/system resiliency is a high priority. These practices are a broad category and encompass several of the other areas. It is not just specific to cybersecurity. Resiliency practices are leveraged to withstand other impactful events such as natural disasters.

ARE SOME OF THESE PRACTICES NOT APPLICABLE FOR BUSINESS OR MISSION NEEDS WITHIN PARTICULAR SECTORS?

There are differences across sectors. While some are unwavering, others allow flexibility. With the Aerospace sector it requires strict compliance without consideration for cost-benefit relief. As a result, there are significant differences in how some of these practices are implemented and enforced. For example, access to aircraft equipment and facilities is strictly controlled through badge reading, personnel checks, and airport physical access control systems. Aircraft incidents are subject to mandated reporting and are subject to investigation by dedicated resources such as the National Transportation Safety Board (NTSB). All avionics are subject to design assessments, testing, and verification requirements.

Within the energy sector, although recommended, some practices are not required or do not apply to all sub-sectors. For most cases, business or mission, a one size fits all is not a reasonable approach and risk based considerations should be part of the solution.

WHICH OF THESE PRACTICES POSE THE MOST SIGNIFICANT IMPLEMENTATION CHALLENGE?

Practice implementation challenges can be grouped into two elements:

- Technology
  - Encryption and key management are challenging. Many legacy devices do not and cannot support encryption. Key management is an ongoing expense due to the lack of policy driven key management systems. Additionally the use of encryption and key management due to the high mobility of aircraft across international legal boundaries can create technical challenges.
- Process / Policy
  - Monitoring & Incident Detection: the threat landscape is continually evolving/shifting, and the technology is expensive and resource intensive to manage effectively. Mission/system

resiliency practices are broader in scope than just cybersecurity which by itself means additional requirements.

- Difference at the international level regarding privacy can pose challenges to sharing vulnerability, threat and resolution information across global entities.

HOW ARE STANDARDS OR GUIDELINES UTILIZED BY ORGANIZATIONS IN THE IMPLEMENTATION OF THE PRACTICES?

For the production and manufacturing of mission level systems all practices are developed for compliance with standards and guidelines. This is also the case in both public and private deployments. In some cases, such as cryptography there is near universal adoption of the NIST cryptographic standard as a best practice.

Non-mission or company enterprise systems utilize a variety of standards in the implementation of practices. Publications such as ISO/IEC 27000-series can serve as a foundation for internal policies & standards that are adapted to address an organization's cybersecurity requirements.

DO ORGANIZATIONS HAVE A METHODOLOGY IN PLACE FOR THE PROPER ALLOCATION OF BUSINESS RESOURCES TO INVEST IN, CREATE, AND MAINTAIN IT STANDARDS?

For program/product needs, methodologies exist and compliance requires the allocation of the appropriate resources to engage and the appropriate investment to be in place. For example, sufficient resources to achieve compliance with standards must be allocated in order to receive and maintain FAA design and operational approvals.

At the enterprise level, different frameworks are utilized in order to make the best use of available resources. Honeywell uses The Unified Compliance Framework (UCF). The UCF maps standards and practices and Government agencies' requirements. In addition, relationships with industry forums are used to validate threats, assess solutions and rationalize security investments.

DO ORGANIZATIONS HAVE A FORMAL ESCALATION PROCESS TO ADDRESS CYBERSECURITY RISKS THAT SUDDENLY INCREASE IN SEVERITY?

For the industrial energy sector and aerospace transportation sector, all incidents which may affect safety margins must be reported. Companies can utilize reporting mechanisms and relationships with threat sharing organizations to allow for sharing of information for severe risks. These kinds of escalations allow companies to more quickly react with product enhancements.

For customers who request continuous monitoring of their critical infrastructure, cybersecurity risk is regularly evaluated at the operational level through recurring audits, risk assessments, incident management and root cause analysis. Much of this can be accomplished in real-time comparing findings against threat levels.

Some escalation processes allow organizations to adjust their security response capabilities to address specific targeted threats. These processes employ a uniform system of progressive readiness conditions ranging from normal to maximum readiness. Linked to each readiness condition are control and response options which can be applied to anticipate and or respond to specific intrusion characteristics or activities.

Findings are formally published in audits and threat briefs and are reviewed and assessed by appropriate stakeholders at formal risk assessment meetings. Additionally, stakeholders are

alerted as part of the response process to any incident with characteristics that could have a material impact on an organization.

WHAT RISKS TO PRIVACY AND CIVIL LIBERTIES DO COMMENTERS PERCEIVE IN THE APPLICATION OF THESE PRACTICES?

This risk is most likely to be realized when work is accomplished across international boundaries. Exposure of personal information can occur for both the victim and the attributed entity. Many industrial energy critical infrastructure systems are focused on commercial and industrial sectors as opposed to residential and consumer sectors. In these commercial and industrial sectors there are limited civil liberties issues when compared with residential and consumer sectors. If an information sharing and analysis center is established for example, then appropriate legal protection must be in place to control the distribution of proprietary information.

For internal storage and management of information at the enterprise level, the boundary between personal & corporate data is shifting. It is common to mingle both corporate & private data on a single mobile device which makes monitoring and responding challenging without infringing on an individual's right to privacy.

WHAT ARE THE INTERNATIONAL IMPLICATIONS OF THIS FRAMEWORK ON YOUR GLOBAL BUSINESS OR IN POLICYMAKING IN OTHER COUNTRIES?

For avionics products, international interoperability and reciprocity means that domestic requirements will be propagated globally. Lack of coordination with other national standards can result in exaggerated compliance costs, outright conflict between other requirements, or being disqualified from certain markets. Within enterprise technology bounds, privacy & encryption are the most difficult areas to address. Each country has unique privacy requirements and laws and varying degrees of acceptance levels of encryption. Enforcing policies & standards across borders becomes increasingly complex.

HOW SHOULD ANY RISKS TO PRIVACY AND CIVIL LIBERTIES BE MANAGED?

Clear boundaries regarding information sharing must be established and agreed upon at the nation state level. If uncoordinated with other national standards, risks can result in exaggerated compliance costs, conflict between other requirements, or being disqualified from certain markets. Internationally accepted standards can ease the conflict, but can take much time in reaching consensus.

IN ADDITION TO THE PRACTICES NOTED ABOVE ARE THERE OTHER CORE PRACTICES THAT SHOULD BE CONSIDERED FOR INCLUSION IN THE FRAMEWORK?

Some recommended inclusions are as follows:

- The framework must not be so narrow that it inhibits innovation.
- The framework should leverage lessons learned from previous efforts and develop an incremental voluntary adoption approach.
- Practices should be based on showing that the security risk of the fielded system and related procedures is acceptable.
- Simple separation of business from operational systems is not correct—operational systems exist fundamentally to support a business and must include interfaces for maintaining and monitoring operational functions, as well as providing data to support other business functions.

ACRONYM GLOSSARY

AC	Advisory Circular
ARP	Aerospace Recommended Practices
ATC	Air Traffic Control
CFR	Code of Federal Regulations
COBIT	Control Objectives for Information and Related Technology
DIACAP	Department of Defense Information Assurance Certification and Accreditation Process
DIB SCC	Defense Industrial Base Sector Coordinating council
DIP	DIACAP Implementation Plan
DoD	Department of Defense
DoT	Department of Transportation
FAA	Federal Aviation Authority
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
ICAO	International Civil Aviation Organization
ICFs	Information Security Forum and Information Risk Executive Council and Network Frontiers
IEC	International Electrotechnical Commission
ISF	Information Security Forum
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
NIST	National Institute of Standards and Technology
NTSB	National Transportation Safety Board
POA&M	Plan of Action and Milestones
RFI	Request for Information
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive/Aerospace Engineers
SEC	Securities and Exchange Commission
SIP	System Implementation plan
SOC	Security Operations Center
UCF	Unified Compliance Framework