National Institute of Standards and Technology Request for Information

"Developing a Framework to Improve Critical Infrastructure Cybersecurity"

The Boeing Company

8 April 2013

Table of Contents

Table of Figures

Introduction

The Boeing Company is pleased to respond to the National Institute of Standards and Technology (NIST), addressing the questions contained in the RFI titled "Development of New Cybersecurity Framework".

We applaud President Obama's Executive Order on Improving Critical Infrastructure Cybersecurity. The strength of our government and our free enterprise system is directly related to the prosperity of our interconnected world. Our businesses and our nation depend on our ability to share the right information, with the right people, at the right time.

Boeing is the world's largest aerospace company and leading manufacturer of commercial jetliners and defense, space and security systems. Our success is based on providing our customers with state-of-the-art products based on our leadership in technology and innovation. Protection of the critical infrastructure and our own intellectual property that creates and sustains this technological leadership is at the core of our efforts and the key to future success.

The critical infrastructure assets and systems we depend on are essential to our way of life. Networks are embedded in our economies and our political and social lives. These networks and information systems hold information of immense value, and they control the machinery that provides our critical services and impact our everyday lives from banking to travel. While this interconnectedness creates immense economic value, we now realize it has the potential of being a major source of risk to commerce and our nation.

Our Nation's critical infrastructure is complex and interrelated. We must understand not only its strengths, but also its vulnerabilities to the emerging threats. In October of 2012, Defense Secretary Leon E. Panetta warned that the United States was facing the possibility of a ***"Cyber-Pearl Harbor".*** We are increasingly vulnerable to domestic and foreign computer hackers who could disrupt the nation's power grid, transportation system, financial networks and government.

Cyber incidents can have devastating consequences on both physical and virtual infrastructure. We must all take responsibility to fortify against cyber risks, improving infrastructure security, and enhancing cyber information sharing between government and the private sector. Physical threats put our Nation's most important assets at risk. Imagine the impact of both a physical and cyber attack? What would 9-11 have looked like with the added simultaneous cyber attack? We must build a workable framework and fortify the partnerships between the USG and businesses in our private sector. We must continue to modernize our critical infrastructure and bolster our ability to overcome whatever challenges we may face. Cyber is not only a national security issue but it is a ***team sport.*** All of us have a part to play in protecting our critical infrastructure and making it more resilient.

Boeing is acutely aware of cyber threats to national and economic security. Boeing's business cuts across several of the 16 critical infrastructures outlined in Presidential Policy Directive 21 (PD-21). We have a very vested interest to ensure that we protect our business infrastructure, our products and services, and ultimately the ecosystem in which our customers use our products and services.

Boeing works tirelessly to defend its information and networks against bad actors. At the same time, there is widespread agreement that the protection and resilience of these systems and assets require the public and private sectors to work together, particularly when it comes to greater sharing of information. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats.

Overall Approach for a Framework to Improve Critical Infrastructure

Boeing believes, as written in the President's Executive Order, that the cybersecurity framework needs to be both risk based and performance based. Risk management is a foundational principle of homeland security. Performance based standards have a well-established history in federal regulatory efforts and should be part of the cybersecurity framework. Performance standards specify the outcome required but leave the specific measures or techniques to achieve that outcome up to the discretion of the regulated entity in partnership with federal entities. We recommend against any attempt to mandate preferred cybersecurity solutions—whether a practice, a process, or an IT product or service—without the consent of affected owners and operators. Top-down approaches to instituting information security measures and controls should not have a place in a genuinely collaborative program.

Boeing believes that a cybersecurity capability maturity model should serve as part of the framework to manage risks to critical infrastructure. Use of a cybersecurity capability maturity model as the overarching structure to reduce risks to critical infrastructure and to implement the cybersecurity program is a sound approach. There is good work already done in the energy sector, specifically the Electricity Subsector who has developed a Cybersecurity Capability Maturity Model, featuring some of the following objectives that could be applied to other sectors:

- Enabling critical infrastructure owners and operators to evaluate and benchmark cybersecurity capabilities.
- Sharing best practices and other relevant information with industry partners as a means to improve cybersecurity capabilities.
- Assisting critical infrastructure owners and operators with prioritizing investments in cybersecurity.

Boeing believes that the cybersecurity framework should closely align with, not interfere with, the enterprise risk-management strategies of critical infrastructure. The cybersecurity framework should not inhibit public-private partnerships. We also believe the cybersecurity framework should not mandate third-party audits. Any auditing procedures should be mutually agreed upon by critical infrastructure professionals and government officials. The EO calls for "measuring the performance of an entity" in implementing the framework. It is unclear if metrics would entail auditing critical infrastructure, such as third-party audits. Boeing is concerned about proposals that call on identified critical infrastructure to be evaluated by a third-party auditor. Complying with third-party assessments would be costly and time consuming, particularly for small and midsize businesses.

Many businesses already have processes in place for assessing and improving the strength of their networks and systems, these mandates maybe unnecessary. Owners and operators in the business community are concerned that the release of proprietary information to the government and third parties could create new security risks. Third-party audits should be optional, not mandatory.

It is imperative that the economics of the framework be considered. "Cost-effectiveness" needs to be a consistent theme throughout the development of cybersecurity framework. Maintaining a cost-effectiveness perspective should be consistent throughout the cybersecurity framework and overall program. The issue of cost may not be an inhibiting factor for some critical infrastructure entities. However, the cost of complying with a "voluntary" cybersecurity framework/program could be a significant issue for some critical infrastructures, and it should not be overlooked. A cybersecurity framework and overall program should be able to measure a covered critical infrastructure's relative gain in security compared with its outlay of resources (e.g., capital, human talent). In other words, owners and operators need to get sufficient bang for the buck.

The framework needs to be developed in a manner that provides critical infrastructure a return on investment. Any cybersecurity program must afford businesses maximum input and flexibility with respect to implementing best cybersecurity practices. Companies have spent millions to protect their IT assets and to enhance enterprise resilience. Any government cybersecurity program that puts claims on private-sector resources must not weaken companies' efforts to keep pace with sophisticated threats. Moreover, a cybersecurity program must not divert companies' resources toward satisfying compliance mandates instead of improving security. Cybersecurity program outcomes that fuel concerns about a lack of ROI would be viewed as unacceptable.

Boeing's Support and Commitment

The Boeing Company is very pleased to support NIST's endeavor of building a cybersecurity framework to improve and ensure our critical infrastructure systems are secure. We are concerned both as an entity interested in protecting our own company, our products, the safety of the flying public and the aviation industry and as a contractor working on cybersecurity for the federal government and other customers. We want to share several key points from our business perspective:

- We believe that all stakeholders need to work together to share cyber threat information and best practices for prevention, detection, removal, and recovery from network attacks until a more secure information infrastructure can be developed and implemented.

- Boeing supports the establishment of standardized Government-Industry non-attributed, non-punitive Cyber Information Sharing forums that minimize the risk associated with self-reporting cyber threats, cyber-breaches and cyber-risk mitigation best practices with appropriate liability protection.

- Boeing supports voluntary cyber threat information sharing with government and private sector entities.

- Boeing supports the creation of industry-led cyber security best practices that result in straight-forward guidelines that insure system critical infrastructure security, employ appropriate self-regulation by industry, and provide industry with liability protection similar to PL 85-804 and Anti-terrorism Technology (ATT) protections.

- Boeing supports efforts to facilitate industry's ability to manage the Insider threat, staying attuned to employee privacy and people risks.

- Boeing supports the creation of industry-led international cyber cooperation with processes and outcomes that are similar and not conflicting with domestic efforts

Information-sharing legislation and other consensus measures would help industry protect America's infrastructure, not more regulation. Boeing supports improving information sharing and liability protection that would put timely, reliable, and actionable information into the hands of business owners and operators so that they can better protect their systems and assets against the increasing threat of cyber attacks. Additionally, businesses need certainty that threat and vulnerability information voluntarily shared with the government would be provided safe harbor and not lead to frivolous lawsuits, would be exempt from public disclosure, and could not be used by officials to regulate other activities. We are committed to working with lawmakers and staff to ensure that the information-sharing process includes privacy and civil liberties safeguards.

Any response to the NIST request should consider existing policies and processes as well as cultural barriers to better integrate and share across historically separated people, systems and institutions. Today's dynamic operating environment will continue to challenge us to keep up with this emergent and insidious threat. The NIST framework to be effective must address the development, integration, and implementation of policy, processes and technologies to secure our critical infrastructure. Additional important considerations include -

1. **Heighten public awareness and education:** Good cyber "hygiene"—or taking relatively simple behavioral precautions, such as keeping antivirus software up to date and backing up files—can reduce a significant percentage of cyber risks to information networks. Legislation should help industry combat much of the nefarious and comparatively unsophisticated activity seen online, freeing up limited human and capital resources to focus on more advanced and persistent threats.

2. **Support greater public-private collaboration:** Businesses are heavily focused on guarding their operations from interruption and intrusion, preventing the loss of capital and intellectual property, and protecting public safety. They devote considerable resources to maintaining their operations in the wake of a natural hazard or man-made threat, such as a cyber attack. Industry expects that the US Government would serve to complement, not harm, the public-private partnerships existing under the National Infrastructure Protection Plan (NIPP) framework

3. **Improve information delivery and access through common standards.** Improving discovery and access involves developing clear policies for making information available not only across all owners and operators but potentially international partners. Secure sharing will relay not only on our best information technology latest technologies in identity, authentication, and authorization controls, as well as data tagging, enterprise-wide data correlation, common information sharing across a wide array of stakeholders.

4. **Shared situational awareness and optimized effectiveness via shared services and interoperability.** Shared situational awareness and timely information sharing is critical and must include focus on optimizing mission effectiveness and increased operational efficiencies to support a viable outcome for all parties.

Boeing would support the creation of voluntary, industry-led, sector-wide best practices to strengthen cybersecurity capabilities across all of industry. All entities, public and private, need to work together and share information in an effort to keep up with the threat, and ideally, get ahead of it. We are currently involved in the available sharing environments with the government, and would like to see these expanded, especially with the addition of liability protection. Several information sharing bills, all broadly supported, have been offered in the Senate and the House of Representatives that would accomplish this.

In addition, Boeing also supports initiatives to increase the ability of an organization to manage insider threats; more robust initiatives to improve international cooperation; and incentives for education, workforce development, and research and development. All of these policies should be crafted with appropriate safeguards for privacy and civil liberties.

In summary, Boeing believes significant progress can be made if government and industry work together. The government should assist private sector efforts by providing incentives, assistance, and liability protections. Companies must be current with state-of-the-art defensive technology, nimble, innovative, and free from unnecessary regulatory interference or restrictions.

Thank you for the opportunity to respond to this strategic framework challenge. Boeing looks forward to working with NIST to address this very important issue.

Organization of the Responses to the RFI Questions

Boeing is committed to working with the administration, lawmakers and industry specific groups to ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats. Enhancing the situational awareness of critical infrastructure owners and operators *would actually increase the security of personal information* that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them**.**

Our response to the NIST RFI follows the RFI questions structure. Section 1 ("Current Risk Management Practices") covers Risk Management, Compliance, 3rd Party Risk, Education, and Portfolio Management. Section 2 ("Use of Framework, Standards, Guidelines, and Best Practices") covers technologies and is organized into six areas: Data Protection, Application Security, Platform Security, Access Control, Intelligence Services, and Resilience. Section 3 ("Specific Framework Practices") covers the adoption of practices as they pertain to critical infrastructure components.

Section 4 provides an in-depth Information Technology response. This Section responds to a more generalized set of questions: 1) A set of questions focused on describing the issues around cybersecurity and how organizations evaluate risk. 2) Questions about existing risk frameworks. 3) Questions focused on existing risk practices.

Best practices, existing standards, and recommendations are listed in their appropriate subject matter area under this taxonomy and are so identified to aid NIST in compilation. These best practices are based on our extensive experience with managing the security services for a large, globally connected enterprise with hundreds of large customer organizations and thousands of suppliers. Most of these represent actual implementations, some represent current projects and directions.

1 Current Risk Management Practices

1.1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

1.1.1. In general for commercial aviation, there are challenges in both the legal framework for sharing both domestically and international with global partners and the economic cost of securing our critical infrastructures that may impact our nation’s ability to be competitive in a global market. Specifically for commercial aviation, the our greatest challenges fall into the following categories:

Understanding of the cybersecurity threats and risks – Commercial aviation has not been impacted as much by cybersecurity threats as other sectors. Therefore, there is a lack of understanding of the threats and vulnerabilities, requiring more cyber education across the commercial aviation infrastructure (airlines, airports, suppliers and regulators).

Speed of change – Aviation has developed a very safety conscience culture that has served itself well over the years resulting in a very safe mode of transportation but one that is highly regulated and slow and conservative when incorporating change. A security culture, while benefiting from the risk management approach taken from the aviation safety culture, will need to be more responsive to the adaptations of cybersecurity threats, requiring much more adaptive solutions in shorter time frames.

Safety vs. security – Many in aviation felt confident that our systems were immune from the cyber attack because of the long and rich history of development and certification of the airplane and airline regulations. There is a widespread opinion that safety management deals with all security issues, but since safety management discounts malicious activity, this is may not always be the case.

Government/Industry sharing of information – Unlike physical security where airport and passenger security and countermeasures can be used to reduce the risk of terrorist attacks such measures have little or no impact on adaptive cyber-attacks. Cybersecurity risk management requires far more emphasis on good system architecture and design as well as targeted, actionable intelligence on threats and intent of those threats. Intelligence sharing of government-to-industry, industry-to- industry and industry-to-government will play a vital role in assessing threat risks and allowing intervention to reduce vulnerabilities.

Consolidation – We are both a global and IT systems dependent enterprise. Our mobility has created increasing interconnectedness and interdependent systems, so organizations are exposed to risks caused by security weaknesses ***in other company's systems***. An airplane goes around the world in less than 24 hours – and can carry bugs (both physical and cyber) that can impact our world. We learned from Stuxnet that industrial control systems are vulnerable, and to put that thought into perspective, our airplane is a global mobile industrial control system.

International cooperation –The airline operators, airframe manufacturers, airports, suppliers, and regulators are global, not based solely in the United States. Timely International sharing of threat information, especially threats that could result in adverse safety consequences, is challenging since exposed vulnerabilities are considered sensitive or even classified, resulting in restrictions to sharing with foreign based companies.

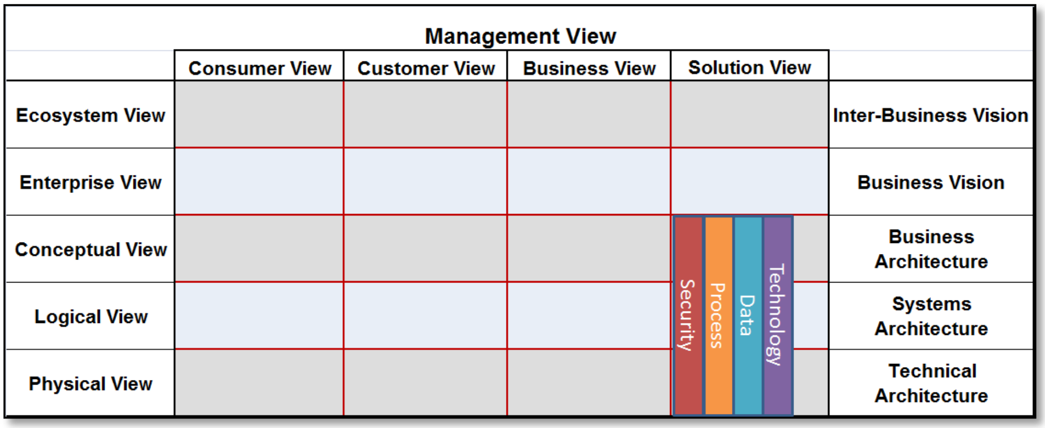
Critical to Cybersecurity is the ability to model proposed technologies and methodologies in a live, virtual, and constructive environment to simulate and analyze their performance. This allows the calculation of industry Key Performance Parameters and measures of performance for their effectiveness under operational conditions. It provides a way to "certify" cybersecurity products and methodologies based on interoperability and effectiveness standards. The Boeing patent Capability-based testing and evaluation of network performance (US Pat 7,894,357) addresses how to measure and test the cybersecurity impact and performance of an architecture design .

1.2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

1.2.1. The greatest challenge in developing a cross-sector standards-based Framework for critical infrastructure deals with the fact that each sector has different mission needs and requirements. Our nation and the critical infrastructures have legal, regulatory, and economic barriers that make cross sector sharing challenging. Some sectors are regulated while others are not and the Framework will have to address both regulated and non-regulated environments. The Framework must ensure flexibility to meet those challenges and yet the depth to tactically deal with a cross-sector standards-based, whole of nation approach.

1.2.2. The cross-sector approach challenge includes the ability to understand the requirements for the approach, the time and effort of defining, accepting and incorporating standards relative to the value derived, and communication between sectors in a timely and effective manner. Cooperation is vital for an effective cyber effort to be deployed and effectiveness maintained. This cooperation includes companies within an industry sector, cooperation of companies between industry sectors, cooperation between government and industry, and having effective legislative involvement that will be an incentive to make the necessary investments to protect critical infrastructure and to discourage indifference to cybersecurity.

1.2.3. The managerial view of Cybersecurity (figure 1) is inclusive of a consumer view, customer view, business view and a solutions view. The consumer view is defined as a view of the business and solutions from the consumer perspective of the product/service provider. These consumer, customer, business and solution views are defined from five perspectives: 1) an ecosystem view, 2) an enterprise or business perspective, 3) a conceptual or business architecture perspective used to communicate concepts and capabilities within the analytical and architecture communities, 4) A logical or systems architecture view that identifies and defines the procedural and functional perspectives and 5) the physical or technical perspective that defines the detailed operational specifications of the system. In the instance of cybersecurity the managerial view framework would enable the decomposition and traceability of the cybersecurity requirements from the enterprise perspective to the operational capabilities.



	Management View				
	Consumer View	Customer View	Business View	Solution View	
Ecosystem View					Inter-Business Vision
Enterprise View					Business Vision
Conceptual View					Business Architecture
Logical View					Systems Architecture
Physical View					Technical Architecture

Figure 1. Cross Sector Ecosystem View of Cybersecurity

1.2.4. The need for a cross-sector approach is reflected in the time and effort of defining, accepting and incorporating standards relative to the value derived and communication between sectors. Historically, years and decades will pass as agreements are defined discussed and adopted within an industry. The need for cross-sector cooperation, outside of common infrastructure service consumption (water, power, fuel, etc.) has been limited.

1.2.5. The greatest challenges to cross-sector standards arise from unique issues and requirements for the various sectors, especially related to government regulation. In aviation, the airplane certification process as well as the requirements for continued operational safety and reporting while the airplanes are operated by our customers is highly regulated. The requirements and operation of the aviation air traffic management system is also maintained by the FAA.

The FAA has provided the aviation industry with a structured hierarchical approach to defining aircraft and aircraft systems. A similar approach will be needed to overcome the communication challenge between industry sectors.

Boeing is committed to working with the administration, and lawmakers and industry specific groups to ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats. Importantly, enhancing the situational awareness of critical infrastructure owners and operators would actually increase the security of personal information that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them.

1.2.6. Framework for Cybersecurity. Many industries have a framework for understanding and communicating information. For example, the FAA has provided the aviation industry with a structured hierarchical approach to defining aircraft and aircraft systems. A similar approach will be needed to overcome the communication challenge between industry sectors.

1.2.7. The separation of business from operational systems; Boeing incorporates both business and operational (e.g., process control) systems into its enterprise. However, Boeing also produces dozens of vehicles (commercial aircraft) each month, each of which incorporates computing capacity in the range of a small- to medium-size business. The configuration of each aircraft, software and hardware, is carefully controlled to its type design and each one receives an individual certificate of airworthiness.

These products are then delivered to customers who incorporate them into their operational infrastructure, including their cyber infrastructure. Each aircraft is certified to meet FAA and foreign authority safety standards. In addition, an increasing number of these aircraft are certified to satisfy cybersecurity standards for safe operation within civilian airspace around the globe.

Product security is thus a key part of Boeing's cybersecurity standards and practices, apart from and in addition to Boeing-owned and operated cyber systems. Boeing is heavily engaged in cybersecurity product research and development, and works with numerous industry, standards, and regulatory organizations to produce development and operational standards and guidance.

1.3. 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?

1.3.1. IT Cybersecurity risk is managed under the direction of the CISO, a VP level position reporting to the CIO. In Commercial Aviation, our Cybersecurity risk is managed under our Aviation Security Director, reporting to a VP level position.

1.3.2. The conventional view of security is primarily aimed at securing an organization's assets, including facilities, goods, IT-infrastructure and information. This self-protecting model has evolved to and necessitates the protecting of the operational environment. This is often referred to as the Aviation Ecosystem (Figure 2).

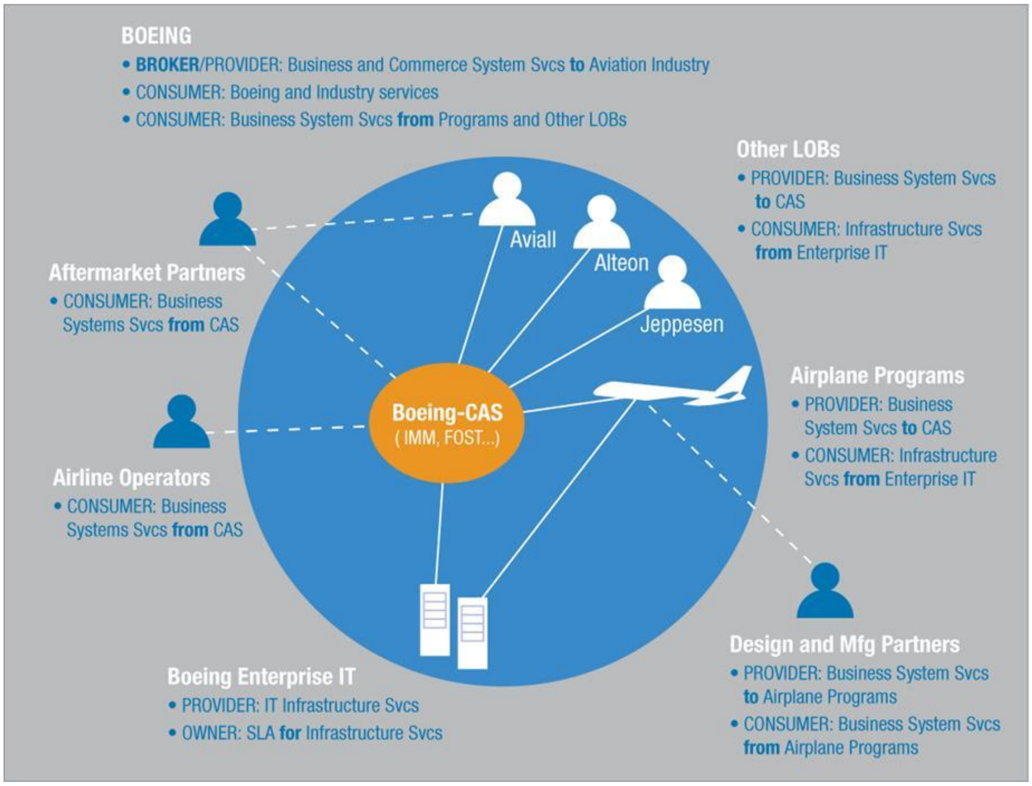

BOEING
• BROKER/PROVIDER: Business and Commerce System Svcs to Aviation Industry
• CONSUMER: Boeing and Industry services
• CONSUMER: Business System Svcs from Programs and Other LOBs
Other LOBs
• PROVIDER: Business System Svcs to CAS
• CONSUMER: Infrastructure Svcs from Enterprise IT
Aviall
Alteon
Jeppesen
Aftermarket Partners
• CONSUMER: Business Systems Svcs from CAS
Boeing-CAS
(IMM, FOST...)
Airplane Programs
• PROVIDER: Business System Svcs to CAS
• CONSUMER: Infrastructure Svcs from Enterprise IT
Airline Operators
• CONSUMER: Business Systems Svcs from CAS
Design and Mfg Partners
• PROVIDER: Business System Svcs to Airplane Programs
• CONSUMER: Business System Svcs from Airplane Programs
Boeing Enterprise IT
• PROVIDER: IT Infrastructure Svcs
• OWNER: SLA for Infrastructure Svcs

Figure 2. Aviation Ecosystem

The actors within the aviation ecosystem have a cohesive interest of ensuring a cybersecurity strategy and framework is continuously operational and that it protects the combined interest of the aviation ecosystem. However, the characteristics of the threat environment that the organizations are exposed to are rapidly changing. Whereas in the past solitary intruders sought entry into a specific organization's network and facilities; nowadays these attacks originate from highly organized groups and are aimed at obtaining services or money by disrupting or diverting the victim's normal business operations. To achieve this, the diversity and sophistication of their means and methodologies has increased drastically from purely IT-based to social engineering, planting a mole or having their own communication device attached to the network. Possible damages for victim organizations could run into millions of dollars or more. The extension of this threat includes disruption to the aviation ecosystem and to other industries that provide support services to the aviation industry. An isolated disruption to the aviation ecosystem would result in tens of millions of dollars daily. A wide spread disruption would result in hundreds of millions of lost revenue on a daily basis

1.3.3. Organizational polices relative to cybersecurity are defined as a function of the Business Continuity Operational Objectives. These business continuity operational objectives are defined as a function of the strategic business vision. See figure 3 below.

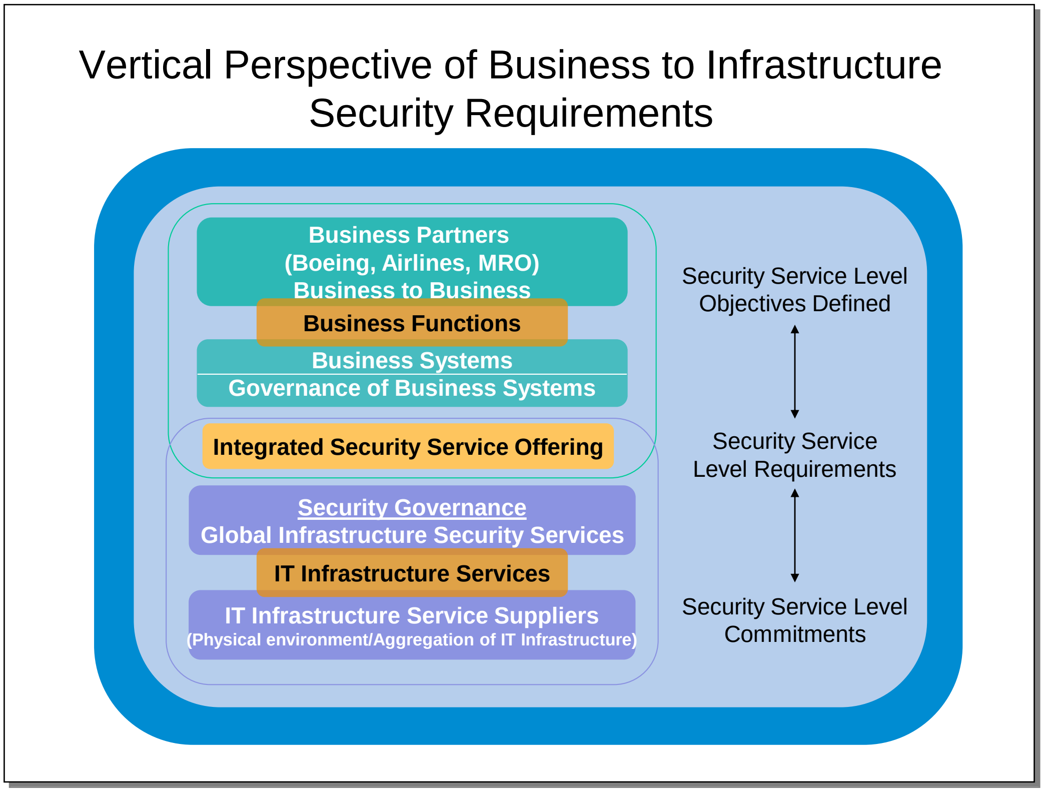

Vertical Perspective of Business to Infrastructure Security Requirements
Business Partners
(Boeing, Airlines, MRO)
Business to Business
Business Functions
Business Systems
Governance of Business Systems
Integrated Security Service Offering
Security Governance
Global Infrastructure Security Services
IT Infrastructure Services
IT Infrastructure Service Suppliers
(Physical environment/Aggregation of IT Infrastructure)
Security Service Level Objectives Defined
Security Service Level Requirements
Security Service Level Commitments

Figure 3. Business Continuity Alignment

1.3.4. Post 9-11, Boeing has invested in a Risk Management Analysis Process (RMAP) technology and Risk Management Analysis Tool (RMAT) for physical security. Boeing is considering how this framework / methodology can be used for aviation cyber security risk analysis and potentially progress into a dynamic cyber defense capability that could remain resilient into the next decade. This framework is initially focused on the aviation sector and may be extended to perform cyber security risk analysis in other sectors, if appropriate. The existing Boeing risk management process, RMAP, is a risk analysis methodology and the RMAT is a simulation tool used by the TSA and industry stakeholders for assessment of physical aviation security scenarios. The RMAT model determines risk reduction for each threat scenario based on an adversary attractiveness and defender consequence comparison between the defined “baseline” system and changes to the system under analysis in the form of alternate defensive countermeasures. The RMAP and RMAT risk assessment methodology is designed primarily for modeling and simulating physical security scenarios and measuring the reduced/eliminated impact of a postulated occurrence. As such, it may not be suitable for assessing cyber threats which require a highly dynamic and agile process that may not be an attribute of the RMAT. This framework and associated methodologies may be able to assess cyber risk, designated as a Cyber Risk Management Assessment Process (CRMAP) and a Cyber Risk Management Analysis Tool (CRMAT).

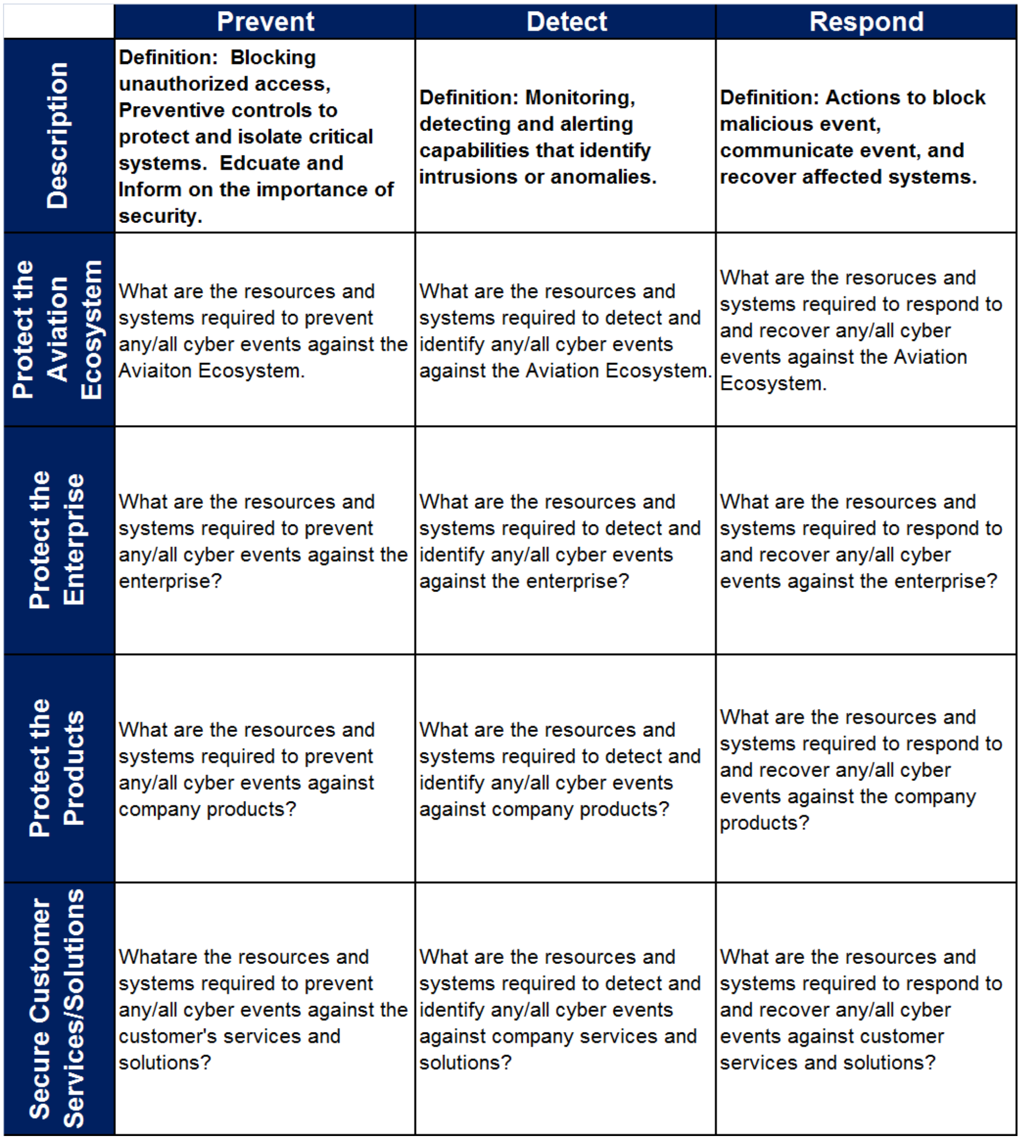
The CRMAP provides the flexibility to develop a rapid, agile, scalable cyber risk management process with an objective of proactively assessing potential cyber vulnerabilities of systems and system of systems. In general the mature Observe, Orient, Decide and Act (OODA) methodology as adapted into the CRMAP provides the ability to meet a variety of needs as the situation requires. The outputs of the CRMAP are:

1. An assessment of potential cyber vulnerabilities and attack surfaces

2. Insights as to an adversary’s threat /attack vectors and preferred methods of attack.

3. An assessment of a change in the risk or risks as cyber risk countermeasures are made to address the vulnerability. This is essentially a repeatable, proactive process to affect an in-depth cyber defense since removing one attack surface could open additional threat opportunities.4. An assessment of the operational and economic impacts associated with cyber risk countermeasures made to defend vulnerability. This allows the customer to prioritize and decide upon actionable options for the design, build and operation of a cyber risk countermeasure

The use of a matrix to define the operational relationship of products to services relative to a Prevent, Detect, and Respond model establishes a concept of a Cybersecurity framework. The first dimension is defined by the hierarchical relationships of the Aviation Ecosystem, the Business Ehe Enterprise Products and the Solutions/Services produced by the enterprise. The second dimension is defined by the enterprise Cybersecurity strategy to: Protect the Business, Protect the Product and Protect the Product Services/Support Services. At the intersection of these two dimensions establishes a point of reference. There are twelve intersection points. There exists an opportunity to define the resources and systems required to enable the required capability at each intersection. Figure 4 is an example of this reference framework.



	Prevent	Detect	Respond
Description	**Definition: Blocking unauthorized access, Preventive controls to protect and isolate critical systems. Edcuate and Inform on the importance of security.**	**Definition: Monitoring, detecting and alerting capabilities that identify intrusions or anomalies.**	**Definition: Actions to block malicious event, communicate event, and recover affected systems.**
Protect the Aviation Ecosystem	What are the resources and systems required to prevent any/all cyber events against the Aviaiton Ecosystem.	What are the resources and systems required to detect and identify any/all cyber events against the Aviation Ecosystem.	What are the resorces and systems required to respond to and recover any/all cyber events against the Aviation Ecosystem.
Protect the Enterprise	What are the resources and systems required to prevent any/all cyber events against the enterprise?	What are the resources and systems required to detect and identify any/all cyber events against the enterprise?	What are the resources and systems required to respond to and recover any/all cyber events against the enterprise?
Protect the Products	What are the resources and systems required to prevent any/all cyber events against company products?	What are the resources and systems required to detect and identify any/all cyber events against company products?	What are the resources and systems required to respond to and recover any/all cyber events against the company products?
Secure Customer Services/Solutions	Whatare the resources and systems required to prevent any/all cyber events against the customer's services and solutions?	What are the resources and systems required to detect and identify any/all cyber events against company services and solutions?	What are the resources and systems required to respond to and recover any/all cyber events against customer services and solutions?

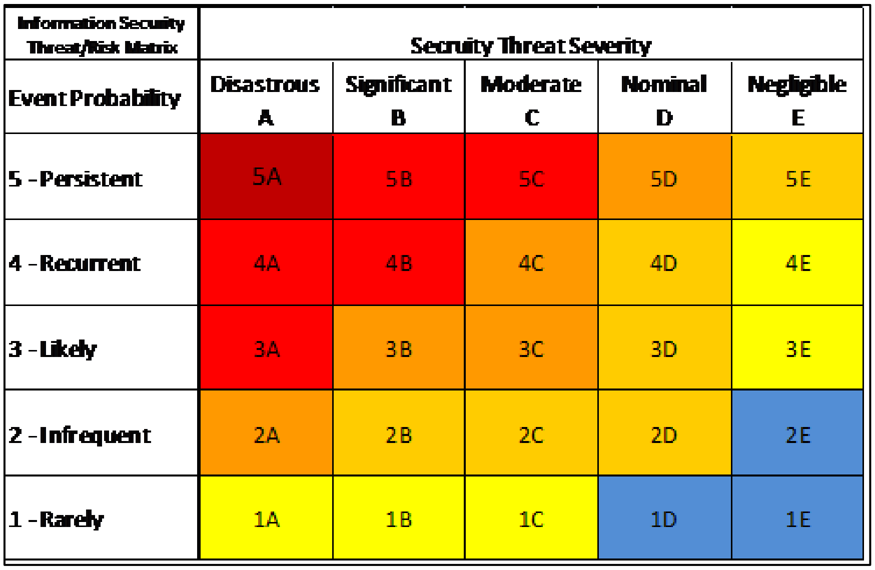
Figure 4. Cybersecurity Reference Framework

1.4. Where do organizations locate their cybersecurity risk management program/office?

1.4.1. The organizational responsibility to ensure proper cybersecurity risk management risk is defined as function of 1) Protecting the Company (Enterprise), 2) Protect the Product (i.e. Airplane) and 3) Protect the Systems and Services utilized by the Customer (Digital Aviation). For example, within the Protect the Product (Airplane) function, the cybersecurity risk management for the airplane architecture resides within the Boeing Commercial Airplane Design Engineering organization.

1.5. How do organizations define and assess risk generally and cybersecurity risk specifically?

1.5.1. Risk Management is a function of understanding (1) the opportunity of disruption to the business, the (2) creditability of the threat, (3) the system or mechanism the threat will be perpetrated upon and (4) the timeliness of the threat relative to the opportunity to prevent or diminish the intended threat. A matrix has been developed to evaluate and characterize security threats following an acceleration and propagation model (see Figure 5). The threat acceleration is an overlooked variable that occurs when a threat event is initiated. The aviation industry, by design, is a well-connected ecosystem. The potential and opportunity for security threats to propagate within this ecosystem is not well defined. A threat acceleration matrix provides an indication of how quickly a security threat may move through the aviation ecosystem. The presumption is that a persistent threat of disastrous consequences would be wide spread and non-responsive to known threat deterrent technology. This type of event would originate or initially be perceived as an infrequent event with nominal threat to the aviation ecosystem. The vertical propagation rate would indicate how quickly the threat would advance to Likely, Recurrent to eventually a Persistent event probability. The threat level would stay constant. However if the threat event had the capability of mutating or to reflect a recombinant capability the horizontal threat severity index would escalate from Nominal to Moderate to Significant. The combination of these perspectives would establish the threat acceleration matrix.



Information Security Threat/Risk Matrix	Security Threat Severity				
Event Probability	Disastrous A	Significant B	Moderate C	Nominal D	Negligible E
5 - Persistent	5A	5B	5C	5D	5E
4 - Recurrent	4A	4B	4C	4D	4E
3 - Likely	3A	3B	3C	3D	3E
2 - Infrequent	2A	2B	2C	2D	2E
1 - Rarely	1A	1B	1C	1D	1E

Figure 5. Security Threat Propagation Matrix

Regarding mission/system resiliency practices; aircraft are designed to be extremely resilient in their ability to safely perform their mission after significant failures. Alignment and integration of cybersecurity design within airplane systems design practices yields similar results for cybersecurity functions, features, and characteristics. Industry best practices are utilized by the Boeing Commercial Airplanes Design Engineering team to perform structured analysis and test methodologies to define, evaluate, and mitigate cybersecurity risk

1.6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

1.6.1. Airplane safety processes in the context of continued safe flight and landing are fundamental elements of our culture. Cybersecurity threats are evaluated in this context.

1.6.2. As described earlier, RMAP and RMAT are developed under our Director for Aviation Security and utilized by our Commercial Airplanes engineering team.

1.7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

1.7.1. Aerospace industry standards are being developed within various industry standards forums to create standards, guidelines and best practices. These elements leverage existing Aerospace standards for safety as well as existing industry cybersecurity standards. The following are examples of industry standards that Boeing adheres to in the manufacturing of commercial aircraft:

1.7.1.1. ADS-B in Security Recommendations (RTCA SC-186 WG4),

1.7.1.2. Aeronautical Mobile Airport Communications Systems (RTCA SC-223) (practice/guideline),

1.7.1.3. NIST Special Publication 800-83, Guide to Malware Incident Prevention and Handling, November 2005.

1.7.2. Boeing is active in developing and securing intellectual property rights and contributing this value to the aviation industry. For example, Patent application # 20120159572 - Method for collaborative rules-based security associated with cloud computing systems. As cloud computing systems become more readily available and demand for cloud computing system services increases, the need for faster, more efficient, and reliable secure access to those services becomes increasingly important. The method uses multiple client profiles, each with one or more access rules. A security logic module receives access request for cloud computing system resources, evaluates the relevant client profile(s) and grants access only to resources allowed by the client profile(s), if any. User access rules may be provided at the infrastructure, network, platform, data and software layers. This novel approach to cloud security is a recommended guideline or best practice.

1.8. 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?

1.8.1. The FAA has 14 CFR Part 25 requirements that require the applicant to ensure the design shall prevent all inadvertent or malicious changes to, and all adverse impacts upon, all systems, networks, hardware, software, and data. There are similar requirements imposed via EASA (European Aviation Safety Agency). The FAA requirements within 14CFR Part 25 encompass elements of the various NIST and industry standards, SP800-30 Risk Management Guide for Information Technology Systems, SP800-53 Information Security, and SP800-82 Guide to Industrial Control Systems (ICS) Security as well as the Common Criteria for Information Technology Security Evaluation. In the context of safety both the operators and the equipment manufacturers are obligated in accordance with 14CFR Part 21 to report incidents associated with their respective safety criteria to the FAA. Aerospace Industry standards are developed via RTCA (Radio Technical Commission for Aeronautics) to address network security as an element of airplane system design specifically RTCA DO-326 Airworthiness Security Process Specification. This standard was co-developed with EUROCAE

(European Organization for Civil Aviation Equipment) and is published in the form of ED-202 Airworthiness Security Process Specification. These standards have been used to support compliance to the requirements imposed by the FAA and EASA.

1.8.2. System and network architecture considerations to support cybersecurity are found in the ARINC 664 series, and in particular in ARINC 664 Part 5. Other Airlines Electronic Engineering Committee (AEEC) communication and equipment standards address security specific to those standards. ARINC has also produced a Technical Application Bulletin (ADN-35A), which provides guidance to ARINC committees to use when producing non-security standards so that security issues are identified and addressed as required.

1.9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

1.9.1. Our business depends on several of the critical infrastructure systems including information technology, telecommunications, energy, chemical, critical manufacture, financial services, water, and transportation

1.10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

1.10.1. Certification to the FAA imposed requirements and continued operational safety are the parameters in which the cybersecurity risk is managed for Boeing Commercial Airplanes.

1.11. 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?

1.11.1. Boeing Commercial Airplanes reports to the FAA on all safety matters and the TSA for security issues. Aircraft are built to public safety and security standards administered by the FAA certification branch and FAA counterparts in each country. Aircraft are operated in accordance with regulations administered by other branches of the FAA, and there are distinct and long-standing roles and responsibilities associated with design and manufacturing versus operations. In general, the same division must hold true for security, because the regulations that address the safety and certification aspects of aircraft will also address the safety aspects of security in aircraft cyber systems. This property must be preserved, because all aspects relating to aircraft safety are ultimately associated with whether an aircraft safely embarks, navigates, and arrives at its destination. Regardless of the threat, the design of the aircraft must ensure proper, predictable, and robust performance when operated in accordance with its requirements.

1.11.2. The FAA sets requirements for safety and, more recently, for product and operational security. New certification regulations are levied by means of Special Conditions on individual aircraft type designs. These Special Conditions require that approved development and analysis processes be followed to assess and address security risks in designs, and that designs include specific features related to cybersecurity. Manufacturers are required to produce operator guidance and recommendations, both for operation and maintenance of cybersecurity on aircraft, and Operational Specifications are issued to require airlines to develop programs to follow the manufacturer guidance and recommendations. Numerous industry bodies provide guidance and recommendations and set standards for equipment, procedures, and processes. These standards form the basis for predictable, interoperable cybersecurity features and functions in aircraft.

1.12. **What role(s) do or should national/international standards and organizations that develop national/international standards play in critical infrastructure cybersecurity conformity assessment?**

1.12.1. National and international standards and the associated organizations are a foundation upon which protection can begin but given the dynamic nature of the threat it is paramount that these standards organization aid in the development of threat sharing information forums as well as formats and reporting context.

1.12.2. In general, a two phased approach should be adopted regarding incorporation of international standards: moving forward as quickly as possible with constructing a framework using domestic standards and best practices (that also leverages international standards and best practices where currently available and stable), but keeping the framework flexible and scalable enough to incorporate future international standards and also be amenable to future harmonization with developing international standards and frameworks.

1.12.3. Significant standards include RTCA DO-326, produced by RTCA Special Committee (SC) 216. DO-326 is a certification process standard for aircraft that are required to address cybersecurity, and is designed to be compatible with SAE ARP4754A which provides safety and certification guidance for highly integrated aircraft and systems. DO-326 is scheduled to be updated to DO-326A, concurrent with the release of an RTCA document addressing cybersecurity assessment methods and a document on maintenance of continued airworthiness for cybersecurity for manufacturers and operators. Once these guidance documents are released, the FAA plans to invoke their use through the issuance of Advisory Circulars, in the same way that RTCA DO-178B guidance is invoked.

1.12.4. Airlines Electronic Engineering Committee (AEEC): produces equipment and process standards for manufacturers and airlines to aid in interoperability and facilitate standards-based approaches. Cybersecurity guidance for airlines is found in ARINC 811: System and network architecture considerations to support cybersecurity are found in the ARINC 664 series, and in particular in ARINC 664 Part 5 Avionics Full-Duplex Switched Ethernet. Other AEEC communication and equipment standards address security specific to those standards. ARINC has also produced a Technical Application Bulletin (ADN-35A), which provides guidance to ARINC committees to use when producing non-security standards so that security issues are identified and addressed as required. The Air Transport Association (ATA) provides cybersecurity standards and guidance for airlines through the Digital Security Working Group to support the use of Public Key Infrastructure technology by airlines. A coordinated activity between ATA and AEEC addresses the use of PKI on aircraft.

1.12.5. We need to ensure any security standards that are created and utilized are interoperable in the global aviation world. Boeing Commercial Airplanes also must follow the International Civil Aviation Organization (ICAO) Standards and Recommended Practices and other pertinent documents. ICAO was created in 1944 to promote the safe and orderly development of international civil aviation throughout the world. It sets standards and regulations necessary for aviation safety, security, efficiency and regularity, as well as for aviation environmental protection.

1.12.6. Boeing Commercial Airplanes is working together with the U.S. Government under the current Department of Homeland Security (DHS) Critical Infrastructure Partnership Advisory Council (CIPAC) program as outlined in the DHS National Infrastructure Protection Plan (NIPP) framework. Following and building on this framework is essential for success. This program has done a good job to date in establishing a risk mitigation approach.

1.12.7. The NIPP outlines an approach that includes actions to mitigate the overall risk to CIKR assets, systems, networks, functions, or their interconnecting links resulting from exposure, injury, destruction, incapacitation, or exploitation. In the context of the NIPP, this includes actions to deter the threat, mitigate vulnerabilities, or minimize the consequences associated with a terrorist attack or other manmade or natural disaster. Protection must include a wide range of activities such as improving security protocols, hardening facilities, building resiliency and redundancy, initiating active or passive countermeasures, leveraging “self-healing” technologies, promoting workforce surety programs, implementing cybersecurity measures, training and exercises, and business continuity planning, among others.

1.12.8. The background specifically of interest to Boeing Commercial Airplanes is Presidential Decision Directive 63 (PDD 63), Critical Infrastructure Protection, intended to assure the continuity and viability of critical infrastructure within the United States. The directive, later updated by the 2003 Homeland Security Presidential Directive 7, mandated that the public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect critical infrastructures within the United States. The mission of the Aviation Sector Coordinating Council (ASCC) is to proactively foster advances in the way the aviation industry, alone and through voluntary interaction with Government partners, provides for critical infrastructure protection for the Aviation Sector of the U.S. economy.

1.12.9. Boeing is pleased to have entered into a Cooperative Research and Development Agreement (CRADA) for Commercial Aviation Infrastructure Security (13-NPDD-006) with the DHS. The purpose of this CRADA is for Boeing and DHS to engage voluntarily in cybersecurity data flow and analytical collaboration activities across the spectrum of cybersecurity coordination including prevention, detection and mitigation.

1.12.10. The purpose of the DHS and Boeing cooperative activities is to share information and develop protocols for sharing information and otherwise collaborate in analyzing such threats and appropriate responses in order to align differing but related missions, business interests, strengths, and capabilities to identify and develop mitigations for emerging cybersecurity risks, thereby enhancing the protection of critical infrastructure and government networks and systems that are vital to National security and the Nation’s economy.

2. Use of Frameworks, Standards, Guidelines, and Best Practices

2.4. What additional approaches already exist?

2.4.1. Boeing has utilized best practices for cybersecurity for decades. These best practices are developed both internally and in discussions with various government organizations, and based on a robust risk management process that incorporates recognized industry and government compliance standards. The principal organizations we work with are the National Institute of Standards and Technology (NIST), the Department of Defense (DoD), and the Department of Homeland Security (DHS). Significant standards we utilize include the NIST 800 series, which was developed for U.S. government use, but is useful for industry as well; Factor Analysis of Information Risk (FAIR), which is useful for categorizing and defining risk; Control Objectives for Information and Related Technology (COBIT); parts of the ISO 27001 Information Security Management System series; Cloud Security Alliance's 3.0 guidance for secure cloud computing; and internet security protocol standards including, but not limited to, communication Transport Layer Security (TLS), Domain Name System Security Extensions (DNSSEC), and Internet Protocol Security (IPSec). All these techniques are continuously updated as threats evolve and technologies change. Our Board of Directors and its Audit Committee are kept abreast of our cybersecurity practices and the threat environment as it evolves.

2.4.2. In addition to our internal networks, our products connect networks for our customers across all domains, providing vital information for the commercial aircraft industry, the intelligence community, the military warfighter, astronauts, law enforcement, and many others. We draw from our internal cybersecurity best practices to secure these networks and utilize the most advanced technical security controls, policy enforcement mechanisms and monitoring systems we can obtain. We work closely with all our customers to ensure we are developing, refining, and employing best practices for protecting critical networks and information systems, and we are continuously updating these best practices.

2.4.3. As cloud computing systems become more readily available and demand for cloud computing system services increases, the need for faster, more efficient, and reliable secure access to those services becomes increasingly important. The method uses multiple client profiles, each with one or more access rules. A security logic module receives access request for cloud computing system resources, evaluates the relevant client profile(s) and grants access only to resources allowed by the client profile(s), if any. User access rules may be provided at the infrastructure, network, platform, data and software layers. This novel approach to cloud security is a recommended guideline or best practice. Patent application # 20120159572 –Method for collaborative rules-based security associated with cloud computing system has been developed in anticipation of the multilevel security requirements cloud services will require to operate securely.

2.4.4. ICAO Aviation Security Manual (ICAO Doc 8973) -- restricted access. Chapter 18 specifically addresses cyber threats to critical aviation ICT systems.

2.4.5. Boeing utilizes the - International Society of Automation Industrial Cybersecurity Standards (ISA-99) for cybersecurity of factory Industrial Automation Control Systems.

2.4.6. Boeing uses the Air/Ground Information Exchange and Manager of Air-Ground Interface Communications (ARINC/AEEC, AGIE/MAGIC) for airspace cybersecurity.

2.4.7. Boeing uses the- Aeronautical Mobile Airport Communications Systems (RTCA SC-223) for Airplane and UAV platform security

2.4.8. The FAA has required that the applicant issue aircraft network security operator guidance (ANSOG) and has required that the operators develop and maintain an Aircraft Network Security Program (ANSP) that documents the operator's compliance to the ANSOG.

2.5. Which of these approaches apply across sectors?

2.5.1. As noted earlier, Boeing Commercial Airplane is working within the CIPAC (Critical Infrastructure Partnership Advisory Council) framework to establish an information sharing forum between the original equipment manufacturers, airline operators, airports, supply chain and other critical aviation partners. Our Boeing Defense team has also been very active with the Defense Industrial Base (DIB) and DIB Collaborative Information Sharing Environment (DCISE).

2.5.2. The FAA, Transport Canada Civil Aviation (TCCA), and EASA participate in SC-216 and WG-72.

2.5.3. A cybersecurity framework needs information superiority in the form of; methodologies and capabilities to convert data into information and knowledge. Boeing has a patent applicable to evaluating network data sensed to detect malware incursions and converting it to knowledge to support forensics and to determine if an attack is under way. System and Method for Controlling Network Centric Operation with Bayesian Probability Models of Complex Hypothesis Spaces (US Pat 8,364,630) discuses a particular algorithm to reduce raw data to information.

2.5.4. A cybersecurity Framework requires information superiority in the form of the ability to sense, characterize, and respond to cyber-attacks while also sharing acquired knowledge with other networks in real time. The following Boeing patents address aspects of this by implementing a geographically distributed free space network architecture:

2.5.4.1. Architecture for Enabling Network Centric Communications, Sensing, Computation, and Information Assurance (US Pat 8,090,264) describes the overarching architecture & subsystems needed to create such networks.

2.5.4.2. Free-Space Sensor Network (US Pat 8,050,568) discusses a geographically distributed sensor network, which is needed to characterize the environment that could be subject to cyber-attack.

2.5.4.3. Network Centric Directed Energy Systems (US Pat 7,999,245) discusses distributed sensor data sources.

2.5.4.4. Multi-Channel Optical Repays for Enabling Networked Communications Systems (US Pat 8,200,09) describes H/W needed within each node to allow the them to connect to one another and create the network being monitored.

2.5.4.5. Methods and Systems for Controlling Storage and Transmission of Data (US Pat 8,370,392) addresses how raw data, which will be monitored to detect cyber-attacks, can be controlled while flowing through the network.

2.5.5. A key issue that can limit of any CyberSecurity Framework is how to assure interoperability and scalability between existing and proposed instantiations of the proposed CyberSecurity framework by members of industry and government. To address this limitation, a hierarchical framework approach is recommended, whereby (1) The top layer would contain definitions of common terms, identification and definition of metrics to be applied in assessing risk and the performance of standards and best practices applied to systems, and core cyber defense standards and principles (best practices) that are generally applicable to all critical infrastructure domains. (2)Lower levels would address similar framework elements (terms, metrics, and standards/best practices) but which are more specific to either groupings of critical infrastructure domains or to individual critical infrastructures. (3) Along another dimension, the framework could be layered according to other criteria such as that found in ISA-62443 (e.g. General / Asset Owner / System Integrator / Component Provider).

2.5.6. Another recommendation is a process that aids in the identification and exploration of the relationships between standards, best practices, laws and regulations, market and domain needs will be useful in both assessing which standards to recommend for inclusion in the framework, and also in identifying barriers to adoption of the framework and underlying standards. Consideration for market forces that motivate and encourage companies to make the needed investments in cyber defense (whether for defense of corporate networks or for defense of their products) should be addressed in this process

2.5.7. A final recommendation would be for a publicly available database of all existing and proposed standards, best practices, laws, regulations, guidelines, and governmental policies will be instrumental to populating, evaluating, and updating the elements of the framework. This database should address all relevant cybersecurity standards, etc., even those whose primary focus may or may not apply to the critical infrastructure domains intended for the framework. This database should include metadata including the standard's identification, owner/controlling organization, region or country, intended domain or application, type (standard, best practice, law, regulation, etc), description, status, and other relevant information. As part of its work with the Network Centric Operations Industry Consortium (NCOIC), Boeing has compiled an initial database with about 300 entries covering standards, best practices, laws, etc that are relevant to cybersecurity for aviation and other domains. While the database is certainly not complete at this point, it does offer a starting point. We suggest that NIST works with an industry body such as the NCOIC to develop and maintain such a database.

2.5.8. If we are developing a joint industry/government CyberSecurity Framework we need to first define an industry/government architecture framework that can be used to harmonize current instantiations in use. There is also a need to establishes a jointly develop set of rules of the road to allow systems developed for industry and governments to interface with each other so they can exchange cyber defense data and cyber capabilities. This is vital to enabling a common and shared cyber defense in this country as well as any other countries that wish to participate in such an integrated cybersecurity framework with us. The above identified cross-sector cybersecurity approaches can be organized and rationalized using a Boeing Integrated Overarching Cyber Architectures Framework. The use of such a Framework can define the limiting requirements that bound the scalability & interoperability between the key capabilities enabled by these core architectures comprising today’s System-of-Systems of networks. The Framework is agnostic; technologies to instantiate a specific architecture to meet a system’s mission goals, while also remaining interoperable within an enterprise cybersecurity Framework, is up to the system designer. These interrelated architectures enable interoperability, as well support self-healing/self-optimizing capabilities, in a fully scalable cybersecurity Framework. The Framework addresses both the instantiating underlying technologies, as well as the policies and business “rules of the road”, that allow for a truly enterprise shared approach. Without a Framework to enable/maximizing sharing of system capabilities, threat data, and current/proposed methods of defense attackers can pick off systems one by one leaving those remaining increasingly vulnerable and isolated as they use the recent successes further hone their attacks in relative safety.

The core concepts serving as the foundation of the Integrated Overarching Cyber Architectures Framework described in (Figure 6) are illustrated by the two dimensional matrix shown in Figure 4 [Cybersecurity Reference Framework] above. The vertical dimension is defined by the hierarchical relationships of the Aviation Ecosystem, Business Enterprise, & Enterprise Products and the Solutions/Services produced by the enterprise. The horizontal is defined by the enterprise Cybersecurity top three strategies to: Protect the Business, Protect the Product, & Protect the Product Services/Support Services. The intersection of these two dimensions establishes 12 points of reference. There exists an opportunity to define the specific resources and systems required to instantiate and enable the required mission capabilities at each intersection.

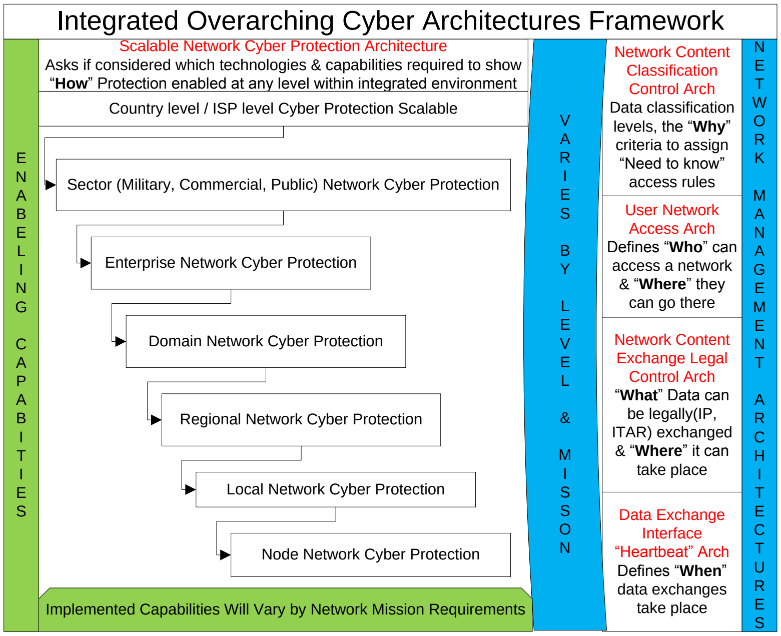

Integrated Overarching Cyber Architectures Framework
ENABELING CAPABITIES
Scalable Network Cyber Protection Architecture
Asks if considered which technologies & capabilities required to show “How” Protection enabled at any level within integrated environment
Country level / ISP level Cyber Protection Scalable
Sector (Military, Commercial, Public) Network Cyber Protection
Enterprise Network Cyber Protection
Domain Network Cyber Protection
Regional Network Cyber Protection
Local Network Cyber Protection
Node Network Cyber Protection
Implemented Capabilities Will Vary by Network Mission Requirements
VARIES BY LEVEL & MISSON
Network Content Classification Control Arch
Data classification levels, the “Why” criteria to assign “Need to know” access rules
User Network Access Arch
Defines “Who” can access a network & “Where” they can go there
Network Content Exchange Legal Control Arch
“What” Data can be legally(IP, ITAR) exchanged & “Where” it can take place
Data Exchange Interface “Heartbeat” Arch
Defines “When” data exchanges take place
NETWORK MANAGEMENT ARCHITECTURES

Figure 6. Integrated Cyber Architecture Framework

A Cybersecurity Framework enterprise should be scalable self-healing/self-optimizing Net-Enabled architectures for agility and resilience as well as information superiority to supply the ability to sense, characterize, and respond to cyber attacks while sharing acquired knowledge with other networks in real time. The availability of methodologies that can serve as standards to enable this means that such a framework can be established much faster. Boeing has three patents for the development of 2nd & 3rd generation that would provide the cybersecurity Framework with the required cybersecurity capabilities, interoperability, & information sharing:

2.5.8.1. Supporting Application effectiveness in a network environment (US Pat 7,817,536)

2.5.8.2. Supporting Effectiveness of Applications in a Network Environment (US Pat 7,929,542)

2.5.8.3. Supporting Network Self -Healing and Optimization (US Pat 7,969,879)

2.6. Which organizations use these approaches?

2.6.1. Airlines for America (A4A) Digital Security Working Group (DSWG) Spec 42

2.6.2. ICAO ATM Security Manual (ICAO Doc 9985)

2.6.3. Low-power Active and Battery Assisted Passive RFID Devices (FAA AC 20-162).

2.7. What, if any, are the limitations of using such approaches?

2.7.1. There is continued development of standards within RTCA and EUROCAE to develop Security Guidance for Continuing Airworthiness and Security Assurance and Assessment Methods for Safety-Related Aircraft Systems. In addition, AEEC produces equipment and process standards for manufacturers and airlines to aid in interoperability and facilitate standards-based approaches. For example, cybersecurity guidance for airlines is found in ARINC 811, while system and network architecture considerations to support cybersecurity are found in the ARINC 664 series, and in particular in ARINC 664 Part 5. Other examples include the Air Transport Association (ATA), which provides cybersecurity standards and guidance for airlines through the Digital Security Working Group to support the use of Public Key Infrastructure technology by airlines, and the Society of Automotive Engineers (SAE) that provides safety and certification guidance for highly integrated aircraft and systems.

2.8. What, if any, modifications could make these approaches more useful?

2.8.1. These approaches to-date have been successful and should not be modified, rather the process should be examined from an opportunity perspective for other sectors to approach protecting their sectors in a similar fashion.

2.9. How do these approaches take into account sector-specific needs?

2.9.1. Due to the regulated nature of our aviation business, we have developed many best practices and standards development processes that may be helpful to emulate in other, less regulated sectors. Examples of guidance that may be useful in other sectors are provided below.

- ICAO Threat and Risk Working Group - Annex 17 and Chapter 18
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Cybersecurity Standard (2006)
- NIST Special Publication 800-85A-1, PIV Card Application and Middleware Interface Test Guidelines (SP 800-73 Compliance)

2.10. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

2.10.1. Boeing encourages a voluntary program. There may well need to be a sector-specific development process that is needed due to issues in that sector as we have outlined above. We encourage steps outlined in the DHS NIPP framework:

2.10.2. Participation in policy development, risk analysis and management framework helps focus both corporate and government planning and resource investment, including:

- Greater information sharing regarding specific threats and hazards enabled by the issuance of security clearances to private sector partners;
- Leveraged application of preparedness guidelines and self-assessment tools within and across sectors so that risks can be managed more effectively and efficiently from the corporate level down to the individual facility level;
- Targeted application of limited resources to the highest risk issues, to include Federal funding where appropriate;
- Coordination and planning across multiple agencies for those assets and facilities that are considered to be at the greatest risk;

- Joint R&D and modeling, simulation, and analysis programs;

- Participation in national-level and cross-sector training and exercise programs, as well as the National Incident Management System;

- Access and input into cross-sector interdependency analyses;

- Established informal networks among private sector partners and between the private sector and the various Federal agencies that can be used for all-hazards planning and response; and

- Identification of potential improvements in regulations.

2.10.3. Government can encourage industry to go beyond efforts already justified by their corporate business needs to assist in broad-scale critical infrastructure protection with incentives and through activities such as:

- Providing owners and operators with timely, accurate, and useful analysis and information on threats to CIKR;

- Ensuring that industry is engaged as early as possible in the development of policies and initiatives related to NIPP implementation;

- Articulating to corporate leaders, through the use of public platforms and private communications, both the business and national security benefits of investing in security measures that exceed their business case;

- Creating an environment that encourages and supports incentives and recognition for companies to voluntarily adopt widely accepted security practices;

- Working with industry to develop and clearly prioritize key missions and enable the protection and/or restoration of related critical infrastructures;

- Providing the resources to enable cross-sector interdependency studies; exercises, symposiums, training sessions, and computer modeling; and otherwise support business continuity planning; and

- Enabling time-sensitive information sharing and restoration and recovery support to priority facilities and services during emerging threat and incident management situations.

2.11. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

2.11.1. Boeing encourages following the DHS NIPP guidelines. Recognizing that each sector possesses its own unique characteristics, operating models, and risk landscapes, HSPD-7 designates Federal Government Sector Specific Agencies (SSA-s) for each of the CIKR sectors. The SSAs are responsible for working with DHS and their respective GCCs to: implement the NIPP sector partnership model and risk management framework; develop protective programs, resiliency strategies, and related requirements; and provide sector-level protection guidance in line with the overarching guidance established by DHS pursuant to HSPD-7. Working in collaboration with partners, the SSAs are responsible for developing or revising and then submitting sector-level performance feedback reports to DHS to enable national cross-sector critical infrastructure protection program assessments.

2.11.2. In accordance with HSPD-7, SSAs are also responsible for collaborating with private sector partners and encouraging the development of appropriate voluntary information-sharing and analysis mechanisms within the sector. This includes encouraging *voluntary* security-related information sharing, where possible, among private entities within the sector, as well as among public and private entities. Consistent with existing authorities (including regulatory authorities in some instances), SSAs perform these activities in close cooperation with other sector partners.

2.12. What other outreach efforts would be helpful?

2.12.1. The Boeing Company has developed and recommended to airlines information security strategies that are focused on continuous improvement to guard against cyber threats. This involves a 6-step continuous improvement information security strategy of setting goals, identifying assets, assessing risk, prioritizing, implementing programs, measuring effectiveness of physical, human, and cyber elements. These are outlined in the 2012 Q3 Boeing AERO magazine article "Securing Airline Information on the Ground and in the Air " (http://www.boeing.com/commercial/aeromagazine/articles/2012_q3/5/)

2.12.2. Boeing Defense, Space and Security programs are engaged with Department of Defense (DoD) stakeholders and customers to better understand their specific needs with regards to cyber risks. Since DoD governance regarding security (and cyber risks) may be different than governance for non-DoD agencies, it should be useful to engage those stakeholders and share information and best practices. For example, Boeing Defense participated in a CRADA, DISA 009-003, known internally to DISA as the Senior Leadership Command, Control, and Communications System (SLC3S) CRADA. The

CRADA discussed using leading governance, performance measurements and static and performance modeling in order to understand and correlate system, operational and environmental performance for senior leader systems. This framework can then be used to modify modeled behaviors across the environment in order to predict future state performance which can then be fed back into the risk management system

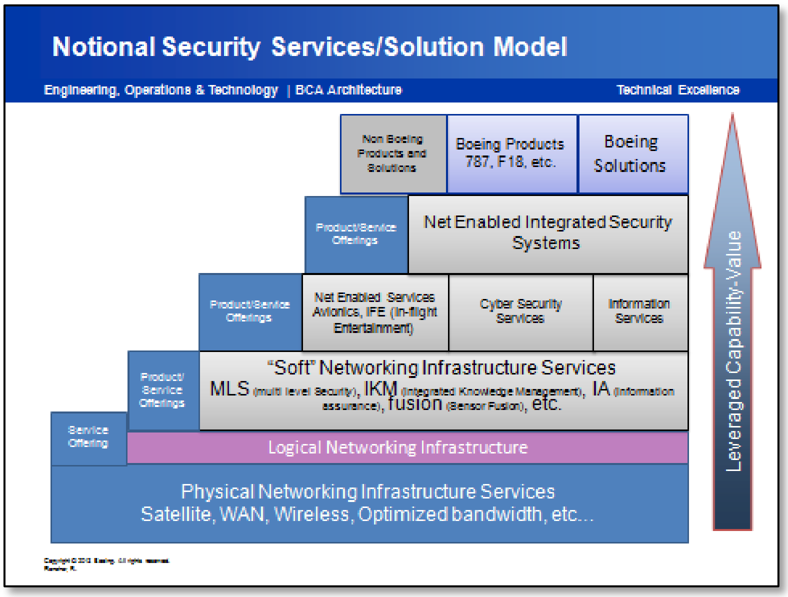
2.12.3. Boeing Defense is observing the NIST family of processes being leveraged in emerging DoD Certifications and IC Certifications. While the NIST governance is useful, it is not always complete when applied to safe guarding classified information. As identified in the above referenced CRADA, reuse of a NIST developed framework would be useful in architecting future state DoD high assurance military grade COTS solutions. Reuse of the framework to identify, analyze and mitigate common threats would provide new design options for the future state systems. By adopting a common framework for developing trusted systems with evaluated products and artifacts, a clear path would be established that encourages the development of composable components with the set of artifacts that support evaluation of the system w/o requiring paid agency support. Ability to get acceptance of an organizations (Boeing) development standards could be a strong motivation for the organization to develop and create solutions

3. Specific Industry Practices

NIST is interested in information on the adoption of the following practices as they pertain to critical infrastructure components:

Separation of business from operational systems;

A services based approach is an effective strategy to enable a cyber-security solution that will address the security challenges of the described aviation ecosystem and related business enterprises. Figure 7 represents a notional layered security services/solutions model that is based upon foundational constructs of establishing securing physical infrastructures services and establishing logical secure services that are then used to enable an integrated service offering based on underlying security services. This approach reduces the practice of designing co-dependent systems that are difficult to re-configure in response to changing cybersecurity requirements and system specifications.



Notional Security Services/Solution Model

Engineering, Operations & Technology | BCA Architecture

Technical Excellence

Non Boeing Products and Solutions

Boeing Products 787, F18, etc.

Boeing Solutions

Product/Service Offerings

Net Enabled Integrated Security Systems

Product/Service Offerings

Net Enabled Services Avionics, IFE (In-flight Entertainment)

Cyber Security Services

Information Services

Product/ Service Offerings

"Soft" Networking Infrastructure Services

MLS (multi level Security), IKM (Integrated Knowledge Management), IA (information assurance), fusion (Sensor Fusion), etc.

Service Offering

Logical Networking Infrastructure

Physical Networking Infrastructure Services

Satellite, WAN, Wireless, Optimized bandwidth, etc...

Leveraged Capability-Value

Figure 7. Notional Layered Security Services Solution

These interrelated architectures enable interoperability, as well support self-healing and self-optimizing capabilities, in a fully scalable cybersecurity Framework. The Framework addresses both the instantiating underlying technologies, as well as the policies and business "rules of the road", that allow for a truly enterprise shared approach. Without a Framework to enable maximizing sharing of system capabilities, threat data, and current/proposed methods of defense attackers can pick off systems one by one leaving those remaining increasingly vulnerable and isolated as they use the recent successes further hone their attacks in relative safety.

Boeing incorporates both business and operational (e.g., process control) systems into its enterprise. However, Boeing also produces dozens of vehicles (commercial aircraft) each month, each of which incorporate computing capacity in the range of a small to medium-size business. The configuration of each aircraft, software and hardware, is carefully controlled to its type design and each one receives an individual certificate of airworthiness.

These products are then delivered to customers who incorporate them into their operational infrastructure, including their cyber infrastructure. Each aircraft is certified to meet FAA and foreign authority safety standards. In addition, an increasing number of these aircraft are certified to satisfy cybersecurity standards for safe operation within civilian airspace around the globe.

Product security is thus a key part of Boeing’s cybersecurity standards and practices, apart from and in addition to Boeing-owned and operated cyber systems. Boeing is heavily engaged in cybersecurity product research and development, and works with numerous industry, standards, and regulatory organizations to produce development and operational standards and guidance.

Use of encryption and key management;

ATA and AEEC have developed guidance and standards for use of Public Key Infrastructure in support of airline business processes as well as for use in aircraft equipment. Due to the nature of aircraft global operations, special considerations are necessary to legally incorporate use of cryptography on aircraft no matter where they are operated. As such, and possibly unique among computer-based products, each individual aircraft must be able to comply with standards in numerous countries at the same time as it flies from one country to another, while a given model of aircraft must be easily adaptable for use by any airline operating within any country in which the model is sold.

Although best available government and public IT practices and standards are the basis from which aviation standards are drawn, aviation regulators, aviation standards bodies and manufacturers are best suited to adapt and develop these requirements and standards for aviation use, including:

- Identification and authorization of users accessing systems;
- Asset identification and management;

Asset identification and management is not a primary aspect of aircraft product security. As befits significant business assets with significant safety regulation and public visibility, aircraft configuration management has always been of high important. However, apart from support for reporting to ground IT systems, is not a significant focus of aircraft cyber security.

- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;

Aircraft are designed to be extremely resilient in their ability to safely perform their mission after significant failures. Alignment and integration of cybersecurity design within airplane systems design practices yields similar results for cybersecurity functions, features, and characteristics.

- Security engineering practices;
- (see discussion above on Special Conditions, RTCA, ARINC, & SAE standards)
- Privacy and civil liberties protection.

See also Section 4

Identification and authorization of users accessing systems;

See Section 4

Asset identification and management;

See Section 4

Monitoring and incident detection tools and capabilities;

A cybersecurity Framework needs methodologies to detect changes in network operational state data for faster and more accurate detection of malware to allow less time detect possible malware attacks and the implementation of defensive course of actions. Boeing as patents specially aligned with this requirement as noted below

Security state vector for mobile network platform (US Pat 8,051,477) focused on monitoring of network security state vector changes

Methods and systems for internet protocol (IP) traffic conversation detection and storage (US PAT 7,995,496) focused on gathering and monitoring of IP data for later forensic analysis

Methods and systems for anomaly detection using internet protocol (IP) traffic conversation data (US PAT 7,903,566) focused on performing forensic analysis on[captured IP traffic data to detect malware

Intentional Data Management (IDM) is an object oriented data integration and management approach applicable to a Cybersecurity Framework developed in BR&T and is currently being used in the creation, management, and persistence of test and analysis data. It approaches data integration at a purely object level using contemporary object design methods, philosophies, and pure object storage for very rapid development, deployment, and modification. The data systems also support multiple languages and SOA from a single object design and compile

Incident handling policies and procedures;

A cybersecurity Framework requires enhanced Knowledge-based capabilities for enhanced data exploitation (from initial point of data collection to downstream forensic analysis). This provides adaptable and repeatable structured forensic analysis of network data to detect cyber-attacks and then chose appropriate courses of action in response. The development and use of key "indicators" is required to perform the forensic analysis with the resulting Knowledge captured in a cyber-knowledge base that is continuously update to fine-tune cyber defense options as well as disseminate the knowledge to other systems. The creation of new cyber-attacks are managed as they emerge.

The release in the Federal Register of the FAA’s Special Conditions for the 787 has resulted in several articles in the mainstream business and technology media speculating on security vulnerabilities of the e-Enabled systems and avionics. This has been compounded by the growing rate of exploitation of Industrial Control Systems which are being increasingly networked and connected to the internet. The risk and collateral damages posed by such vulnerabilities have been exemplified by the introduction of the Stuxnet Worm to attack nuclear production systems in Iran.

In response to this momentum, our BCA Network Security Team has developed an Incident Response Plan (IRP) for airplane information systems and related interfacing systems. The IRP sets forth processes and procedures which minimize both the financial and operational impact of any of the situations regarding e-Enabled airplanes that result from either a credible or non-credible threat or vulnerability.

Mission/system resiliency practices;

Boeing has built, prototyped, and demoed to the Air Force, a Service Oriented Architecture framework, "Integrated Command and Control enterprise" (IC2E) and an application, Dynamic C2ISR Asset Manager (DCAM). DCAM is made up of Services running as a 'thin client' in a web browser using Cursor-On-Target protocol for platform communication & command. It was developed using mostly commercial off-the-shelf (COTS) products and open source SOA to create a flexible design that could be developed in an agile environment.

Development of a Joint Architecture Standard (JAS) for designing of network communication capabilities based on COTS hardware rather developing DoD specific products from scratch is more efficient, reliable, and inexpensive. LANL has already designed and deployed space assets in an 18 month time frame using these technologies.

Leveraging BMA's Digital Eco System with the Navy's Open Architecture and the DoD’s Open Systems Architecture could produce an industry standard Extendable Core Architecture System based on a set of interoperable H/W and S/W options. This could be used to build “plug and play” systems that would allow the use of different types of cybersecurity technologies to be loaded on to networks platform and have instantaneous access to the equivalent capabilities on other networks in the Enterprise.

It may be worthwhile to review a technical adaptation of the OODA Loop. The OODA Loop model was originally developed by Col. John Boyd, USAF (Ret) during the Korean War. It is a concept consisting of the following four actions:

- Observe
- Orient
- Decide
- Act

This looping concept referred to the ability possessed by fighter pilots that allowed them to succeed in combat via a rapid and agile decision process. The OODA Loop is now used as a standard framework or methodology by military, federal and commercial entities as a basis for rapid and continuous assessment and decision making. The premise of the model is that decision-making is the result of rational behavior in which problems are viewed as a cycle of Observation, Orientation (situational awareness), Decision Making, and Action. Boyd diagramed the OODA loop. The OODA loop is discussed here because it is a widely recognized process used in day-to day operations by many organizations, only it may not called out in these exact terms. It described to help start a discussion on the need for a standard set of terms acceptable to both government and industry for a similar approach that can be associated with the cybersecurity Framework.

Security engineering practices:

The Boeing Company is proud of our engineering culture and expertise. We have developed and implemented a Systems Engineering Best Practices (SEBP) across our enterprise. Our goal is to achieve exceptional product and program performance with superior execution of SE throughout the product life cycle and the product supply chain. SEBP is one of the foundational elements to provide superior products and services. Process implementation guidance for SEBP assessments is documented in BPG-08-10001, Assess a Program Using Systems Engineering Best Practices (SEBP) Method.

The SEBP implementation model provides a framework to achieve SE excellence. The model evaluates a program's execution of each best practice by the five component areas of process, tools, implementation, cross-practice integration, and environment. The model shares a common structure with other Boeing best practice models and integrates security into the practice.

Additionally, BCA has a Procedure (PRO83) entitled BCA Engineering Responsibility, Accountability, and Authority (RAA). This procedure describes the requirements, working relationships, and associated responsibilities for Engineering in support of Boeing Commercial Airplanes (BCA). This procedure states that we will “define, produce, and support in a working together environment with clearly defined roles and responsibilities.” The engineering RAA assignments for employees in any of the Engineering skill codes or producing Engineering products and services are documented in this procedure.

Privacy and civil liberties protection:

DHS privacy and civil rights officers should assess annually the EO and recommend ways to minimize impacts on personal privacy. The program should be evaluated against Fair Information Practice Principles and other privacy policies. Boeing is committed to working with the administration and lawmakers to ensure that information sharing includes privacy and civil liberties safeguards. While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats.

Importantly, enhancing the situational awareness of critical infrastructure owners and operators *would actually increase the security of personal information* that is maintained on company networks and systems. Improved information sharing would benefit individuals' privacy protections, not detract from them.

3.4. Are these practices widely used throughout critical infrastructure and industry?

Yes in different parts of our Company and with some of our customers

3.5. How do these practices relate to existing international standards and practices?

- Aeronautical Systems Security - Security Airworthiness of Commercial Aircraft (RTCA SC-216) is a recommended practice

- Passive RFID Tags Intended for Aircraft Use (SAE AS5678)

- ADS-B In Security Recommendations (RTCA SC-186 WG4)

- Boeing Customer Integrated environment - NIST Special Publication 800-82 (Final Public Draft), Guide to Industrial Control Systems (ICS) Security, September 2008.

3.6. Which of these practices do commenter's see as being the most critical for the secure operation of critical infrastructure?

In aviation, we have governments, airline operators, airports, and manufacturers from across the globe that must work together to thwart this threat. It is critical to provide shared situational awareness across multiple stakeholders operating globally to enhance security and ensure resilience.

3.7. Are some of these practices not applicable for business or mission needs within particular sectors?

Yes, many of the aviation specific practices are for aviation only and similarly for the defense sector.

3.8. Which of these practices pose the most significant implementation challenge?

One of the challenges is sharing with our international partners' timely and critical information to thwart the threat. Over classification of information provides challenges in sharing even with our nation's partners and does not allow sharing with our trusted global partners.

Slow moving change environment:

The aircraft industry is a very “highly regulated” industry. To effect changes that would be easily adaptable to the increased cyber threats takes time and makes agile or rapid changes to threats very hard to implement.

Aviation is “safety focused”:

This requires detailed analysis and testing to insure the aircraft have been rigorously vetted not only in their physical development but also in their software code. Any changes to the various base codes require exhaustive analysis and review prior to implementation. This lengthy process will slow the reaction to and solution implementation of a cyber threat.

Catastrophic failures have significant impact:

Whenever there is a major accident, failure, or incident much attention is given to discovering and correcting the root cause. If the cause is a design flaw this will be a top priority for correcting and implementing a fix. Discovering the source of a cyber-attack and how to correct it may be very difficult to find and fix. It is important to fully test and re-test code to ensure that the primary development or function has not been compromised by a cyber-threat.

Broad spectrum of technology deployment throughout the fleet:

We have moved from analog to digital aircraft in the last several decades. To expand the service life of the older legacy aircraft they have been modified and engineered with elements of electronic capabilities. Many of these have “bolt on” capabilities joining with existing infrastructure. Managing across the various e-enabled capabilities brings different threats and protective measures for the various systems.

Siloed components within aviation domain:

No one has the whole picture or understands relationships. Most of the developed E-systems are focused on their requirements and what their functionality needs to be. These can be looked upon as “standalone systems”. They can be considered independent but when eventually joined or interconnected with other E-Systems they become a system-of-systems. This siloed view is also magnified by the number of suppliers and how they are contracted for specific deliverables that may or may not connect with other systems.

Very extensive and growing supply chain:

Boeing has a vast array of suppliers (over 7,000) providing services and parts. These do not all supply cyber parts; however, the number of cyber related parts has increased exponentially with the new generation and legacy airplanes that are now e-enabled.

Limited span of control for Boeing:

Boeing has documented what is recommended to support the aircraft but they have no enforcement capability to ensure their recommendations are implemented.

Span of aviation is global:

Many different agencies and services interface with the aircraft and each has the potential of compromising the systems on board the aircraft.

Wide diversity of cyber system:

Our nation has an old air traffic management (ATM) system – The current ATM structure is very old and the cyber technology and interfaces need to be upgraded and strengthened for cyber vulnerabilities. Old aircraft or legacy aircraft have limited and basic e-enabled capabilities while new aircraft have current state of the art e-enabled systems. This diversity creates potential risks in the aviation cyber domain that are not easily or affordably mitigated.

3.9. How are standards or guidelines utilized by organizations in the implementation of these practices?

Sharing with our international partners. Implementation of the Nation's critical infrastructure protection mission depends on the ability of the government to receive and provide timely, actionable information on emerging threats to owners and operators and security professionals to support the necessary steps to mitigate risk.

Each sector has diverse approaches to establishing their own sectors' information-sharing programs that will most effectively and efficiently meet the requirements of their industry structures, operating cultures, and regulatory regimes. Each sector has the ability to implement a tailored information-sharing solution working in concert to expand the flow of knowledge exchange to all infrastructure owners and operators.

Information Sharing and Analysis Centers (ISACs) provide a recommended example of a private sector information-sharing and analysis mechanism that may be able to address this challenge. ISACs are private sector-specific entities that advance physical and cyber CIKR protection by establishing and maintaining collaborative shared situational awareness for operational interaction between and among members and external partners. ISACs, as identified by the sector's SCC, typically serve as the tactical and operational arms for sector information-sharing efforts.

ISAC functions include: supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with the appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness.

3.10. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

See Section 4

3.11. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

See Section 4

3.12. What risks to privacy and civil liberties do commenter's perceive in the application of these practices?

While personal privacy must be adequately guarded, improved information sharing should aim to enhance situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats. This is a balancing act. The cybersecurity framework must be open to public review and comment. Transparency is key - we urge the NIST to consider how it plans to balance two competing and necessary goals—openness and security.

3.13. What are the international implications of this Framework on your global business or in policymaking in other countries?

Boeing is a global company and cumbersome restrictions or burden on our business could impact our competitiveness in a global market etc.

3.14. How should any risks to privacy and civil liberties be managed?

Privacy and civil liberties must be carefully managed by all parties. Any Framework must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people. The Framework must balance and operate in a manner that advances national security while protecting the freedoms, civil liberties, and privacy rights guaranteed by the Constitution and federal law.

3.15. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

A cybersecurity capability maturity model could be used as the overarching structure to reduce risks to critical infrastructure and to implement the cybersecurity program. It should feature some of the following objectives, could be applied to other sectors:

- Enabling critical infrastructure owners and operators to evaluate and benchmark cybersecurity capabilities.
- Sharing best practices and other relevant information with industry partners as a means to improve cybersecurity capabilities.
- Assisting critical infrastructure owners and operators with prioritizing investments in cybersecurity.[1]

At present, using a maturity model seems like a constructive approach. However, the cybersecurity framework should closely align with, not interfere with, the enterprise risk-management strategies of critical infrastructure. The cybersecurity framework should not alter public-private partnerships, standards program and similarly situated arrangements, without the mutual consent of all parties.

Any cybersecurity program must afford businesses maximum input and flexibility with respect to implementing best cybersecurity practices. Boeing is concerned about a well-intended government program that would become slow, bureaucratic, and costly relative to businesses' need for a qualitative and quantitative return on investment (ROI).

Companies have spent millions to protect their IT assets and to enhance enterprise resilience. Any government cybersecurity program that puts claims on private-sector resources must not weaken companies' efforts to keep pace with sophisticated threats. Moreover, a cybersecurity program must not divert companies' resources toward satisfying compliance mandates instead of improving security. Cybersecurity program outcomes that fuel concerns about a lack of ROI would be viewed as unacceptable.

The following material was prepared by our Boeing IT team led by our Chief Strategist, Steve Whitlock of the Information Security Team

3. General Questions from the RFI

1. What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?

- **Inertia** – The operational difficulty of migrating infrastructure, systems and software to newer versions that have better security. This includes application compatibility – many line of business applications are predominately funded and prioritized for initial functionality without adequate plans for future migration to new platforms. In addition, corporate response to the value of information has lagged. Many organizations see information and IT services as costs rather than business advantages and, as a result, have not made systemic changes that would significantly improve cybersecurity. Instead they have tended to make slow, evolutionary improvements. Recent publicity around cyber-attacks and data theft has improved the awareness of the risks, but attack capability continues to outpace remediation.

- **Affordability** – The inability for an established enterprise to bear the financial cost of periodic wholesale replacement of its IT infrastructure, systems and software. These costs are not limited to software or hardware but also include deployment efforts, testing, end user training, and the effects on the enterprise of running multiple concurrent implementations during any migration.

- **Trust** – The shift from monolithic corporations towards virtual enterprises coupled with extensive outsourcing, extensive supply chains and partnerships has created unstable business trust relationships with shifting loyalties. Additionally, these complex relationships form interwoven trust chains that are susceptible to penetration at their weakest links. As one organization improves security, their attackers simply compromise a partner, customer, or supplier and leverage the trust relationship to gain access. Recent examples include the compromise of the RSA Token software and Gmail, but this is an escalating trend.

- **Usability** – New generations of security technology often strain users with unnatural tasks that have inconsistent interfaces. As an example, while a driver does not need to know how to rebuild a car engine, but rather should focus on operating the car and the rules of the road; a computer user should not have to be a computer security expert but should be able to perform necessary tasks safely by following basic principles. As an examples, the very qualities that make passwords or PINs strong (complexity and length) make them harder for their users to remember. As another example, when confronted with a web site that uses an unknown PKI Certificate, the user gets a pop-up window asking for a trust decision. This is not a decision that a user – or even a security expert – can make without significant investigation, and yet this happens during the normal workflow.

- **Scalability** – The difficulty in extending security best practices across a diverse set of customers and suppliers, each of which has a different level of IT maturity. This is more difficult with smaller organizations that do not have established security or even IT organizations. It is often the case that the immense scale of our infrastructure breaks the first several iterations of many/most vendor products. Frequently, we have to tutor these vendors in how to improve the scalability of their products so that they could be deployed within Boeing.

- **Technology Limitations** – Boeing frequently finds itself trying to secure critical infrastructure before anybody else (e.g., forward proxy, reverse proxy, Identity Management and Federation, supply chain security, cyber—physical security (e.g. Industrial Control Systems)). We therefore often have to invent these security solutions ourselves. Because we are not security vendors, we introduce our inventions to standards bodies so that vendors could adapt those ideas and create them into products. This is partially why Boeing has been very engaged in numerous standards bodies. Unfortunately, standards work takes time, so much so that we often have to create and deploy our own solutions ourselves. This means that we bear the financial burden of doing this development work and then maintaining our inventions over time, when our preference would be to buy vendor security products that the vendors maintain. We then face the additional expense of replacing our solutions by vendor solutions once the latter finally become mature enough – years or decades later.
    - -- A major security problem which we are currently confronting is how best to secure critical data as close to the data as possible. We've investigated several vendor products which would improve the situation but none of them were mature enough to be deployable.
    - -- Another major technology limitation is how to create an enterprise cyber command and control center enabling real time cyber situational awareness and response.

- **Vendor Product Non-Interoperability** – Another reason Boeing spends so many resources in standards bodies is to ensure that the security standards themselves can satisfy our requirements. This is done because vendors have a natural tendency to create products that don't play well with others, thereby creating vendor-lock-in for their customers. We require standards-based solutions so that vendor competition would improve the technology over time in a manner that is interoperable, so that we can more easily deploy the best solution available. We also find ourselves running products long after they have been discontinued or the vendor has gone bankrupt. Interoperability reduces the cost of replacing these products.

2. What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?

- Sector maturity varies. The factors listed in response to the above question (inertia, affordability, and scalability) will affect each sector differently. Sectors that are least prepared will perceive attempts to improve their security as more invasive than sectors that have more mature security best practices.

- Sectors differ in their use of technology. Some sectors may perceive themselves as different enough from others that common sets of best practices and standards should not apply. With the migration of communication systems from proprietary networks to IP, the replacement of specialized IT systems to COTS, and the attachment of industrial control systems to those networks, differences are becoming less and less. Attacks easily cross these boundaries and while there will be some differences the case for a general framework gets stronger as time goes on. A well thought out general purpose framework and set of standards – that has options for specific use cases should be generally applicable. Once this is done, the solution to the perception issue is most likely a marketing effort to convince them that differences are more perceived than real.

- Inadequate standards framework for security interoperability. Several very promising security standards exist (e.g., IETF, TCG, OASIS) but thus far the vendors have incomplete support for these standards, which creates implementation holes when we try to deploy them. Many products are also immature, which introduces scalability and performance issues, making their deployment high maintenance for us.

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?

- The information security program receives authority from corporate policy on information resources through the procedure on information protection, which establishes authority for computing security requirements and standards. An information protection governance board composed of information stakeholders oversees maintenance and implementation of these policies and procedures.

- We have created a security domain model which orchestrates and coordinates our approach. This includes:
    - Operational services: investigation and response (e.g., forensics); monitoring and threat detection (analytics, correlation, IDS, logging); portfolio management (e.g., project prioritization, patch management, product lifecycle management, roadmaps); governance, risk, policy and compliance; and vulnerability assessments.
        - Our perception is that Boeing's emphasis on vulnerability assessments is unusual for most enterprises today. Thus, we will highlight it now: This organization inventories our infrastructure and those with whom we have major dependencies (subsidiaries, suppliers) in order to identify, document, and track security vulnerabilities that can be exploited by advanced persistent threats (APTs) or other sources of attack against computing infrastructure, applications, data or information processing facilities on which Boeing depends. It does penetration testing and assessments (site, network, server, application). The Vulnerability Assessment organization is also responsible for monitoring and tracking corrective actions associated with vulnerabilities identified during the assessment process. The security vulnerability information found by Vulnerability Assessments is consumed by other elements of the IS Domain Model including 1) Governance, Risk, Policy, and Compliance; 2) Monitoring & Threat Detection, and the cyber defense element that is affected by a specific vulnerability (e.g., Access Control Services, Directory Services, Secure Design and Development, and Protection Services).
    - Protection Services: application protection (e.g., firewall, hardening, signing), client protection (e.g., anti-spam, anti-spyware, health check, port and device control), data protection (encryption, data loss prevention, digital rights management, signing and labeling), host and storage protection, and network protection (e.g., enclaves, gateways and proxies.
    - Access Control Services: identity management; authentication; and authorization.

  - Secure Application Development.

4. Where do organizations locate their cybersecurity risk management program/office?

- Cybersecurity risk for our internal network is managed under the direction of the CISO, a VP level position reporting to the CIO. Cybersecurity risk for our products and services are managed by the respective business unit Chief Engineer's office. Cybersecurity risk for our extensive supply chain is jointly managed by the business Unit VPs for Supply Chain Management through a common risk management approach.

5. How do organizations define and assess risk generally and cybersecurity risk specifically?

- A corporate level board risk management board oversees the management of enterprise level risks. Cybersecurity risks are defined in terms of assets (e.g. intellectual property) and threats (e.g. insiders). The risk analysis is based on identified vulnerabilities and the effectiveness of associated controls.

- The cybersecurity risks are included in the status to the corporate risk management board.

- Boeing actively participates within several information sharing and analysis center (ISAC) activities (e.g., DoD, Aircraft products). These intelligence briefings inform our awareness of cybersecurity risk. Intelligence from others is supplemented from our own internal security intelligence processes that are conducted by our internal monitoring and threat detection organization and our vulnerability assessment organization, which was highlighted in our answer to the third question above.

- The National Council of Information Sharing and Analysis Centers (NCI) aids in the coordination of cross-sector efforts with the recognized critical infrastructure sector ISACs, and helps to establish mutual policies and issues that need to be communicated with each of the sectors and the government. When considered collectively, individual private/public sector ISACs represented within the NCI provide an outreach network to approximately 85% of the U.S. critical infrastructure.

- Department of Defense - As a member of the Defense Industrial Base, Boeing participates in the OSD CIO Defense Industrial Base Cybersecurity and Information Assurance Program to assess risks to its Defense Programs and to detect risks that are specifically concerned to the Defense Sector. The DIB CS/IA Program is a collaborative information sharing partnership between industry and the U.S. Government. The goal of this program is to protect sensitive unclassified DoD program and technology information resident on, or transiting, DIB unclassified networks. Key elements of the program include;
  - DCISE - The DoD-DIB Collaborative Information Sharing Environment (DCISE) supports referrals of intrusion events on DIB unclassified corporate networks. The DCISE works with government and industry partners to produce cyber threat reports, which provide threat warning information, report cyber incidents, and contributes to cyber damage assessments.

- Policy and Operations Working Group (POWG) - The Policy and Operations Working Group meets quarterly to discuss policy and operational issues related to the DIB CS/IA program.
- Technology and Architecture Working Group (TAWG) - The Technology and Architecture Working Group meets periodically to discuss technologies/architectures to support improved information security/assurance.
- Other key DoD organizations for assessing risk and coordinating industry responses include:
    - DoD Damage Assessment Management Office (DAMO) Program: The DAMO Program coordinates the impact assessments involving the loss of Controlled Unclassified Information (CUI) resulting from the illicit exfiltration of technical and programmatic data maintained on unclassified Defense Industrial Base (DIB) networks. Boeing provides case data and technology impact assessments to DAMO as required.
    - Defense Security Service (DSS): DSS provides security oversight for the protection of U.S. and foreign classified information and technologies in the hands of industry under the National Industrial Security Program (NISP) and serves as the DoD functional manager for education, training, and professional development of security professionals for the DoD, federal government, and industry.
    - Department of Defense Cyber Crime Center (DC3): DC3 provides digital evidence processing, analysis, and diagnostics for DoD investigations requiring computer forensic support, and assists in criminal, counterintelligence, and counterterrorism.

- Department of Homeland Security - Within the Aviation Sector, as a subset of Transportation, the Department of Homeland Security, National Protection and Programs Directorate (NPPD) plays a major role in determining and assessing risk to our Aviation programs and platforms. NPPD is the proponent organization for a new Government Coordination Council being formed for the Aviation Information Sharing and Analysis Center (Aviation – ISAC) that Boeing will participate in.

- Also within the NPPD, the National Cybersecurity and Communications Integration Center (NCCIC) is responsible for the production of a common operating picture for cyber and communications within the National Protection & Programs Directorate (NPPD. The NCCIC is further enabled in its missions by being collocated with US-CERT and the Industrial Control System Computer Emergency Response Team (ICS-CERT) and direct liaison ties to 7 other US Government Cybersecurity centers.

- Transportation Security Administration **-** The TSA Assistant Administrator and Chief Information Officer leads TSA's IT office with an annual budget responsibility of nearly $400 million. The TSA CIO is responsible for developing and managing central policies for all of TSA's IT requirements as well as developing and implementing IT initiatives across TSA. The Transportation Security Administration (TSA) is authorized by federal statute to promulgate physical security and cybersecurity regulations relating to securing US transportation infrastructure (including aviation, rail, highways, and pipelines).

- Department of Transportation, Federal Aviation Administration **-** The Federal Aviation Administration is a key stakeholder and partner in developing and ensuring the secure operations of Boeing aircraft as they operate in US airspace and with FAA regulated airport facilities. One element for Boeing in terms of risk management is the need to expand ties to the FAA Cybersecurity Management Center in Leesburg, VA, that also manages cybersecurity for the Department of Transportation at large.

6. To what extent is cybersecurity risk incorporated into organizations' overarching enterprise risk management?

- Our governance, Risk, Policy and Compliance organization receives current risk information from intelligence combined with our internal threat detection and vulnerability assessment organizations. These inform the activities and priorities of our various operations and security protection organizations.

7. What standards, guidelines, best practices, and tools are organizations using to understand, measure, and manage risk at the management, operational, and technical levels?

- At the internal network technical level, FAIR (Factor Analysis for Information Risk) is used to identify risk components, COBIT and ISO 27001 are used to capture risk compliance and maturity. For our Products and Services and Supply Chain, Boeing utilizes a proprietary risk management process that closely mirrors DODI 4001 and ISO 9001.

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?

- Boeing tends to focus on Department of Defense requirements for its cybersecurity compliance and threat mitigation efforts. As a voluntary participant in the OSD CIO Defense Industrial Base Cybersecurity/Information Assurance Program and its existing Framework Agreement and Interim Federal Rule, Boeing actively shares cybersecurity incident information with the Department of Defense and its Defense Industrial Base Partners.

- Additionally, Boeing has contractual obligations under OSD AT&L to share information with the government on any cybersecurity related incidents and/or report any damage or leaks of government technology or other critical programmatic information in impacts to Department of Defense Programs in a program managed by the Damage Assessment Management Office (DAMO, under OSD AT&L.

- Finally, the Security and Exchange Commission's Corporation Finance Disclosure Guidance dated October 13, 2011 requires registrants to **"**address cybersecurity risks and cyber incidents in their Management's Discussion and Analysis (MD&A) section if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition"... "If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's 'Description of Business.'"

- In addition to existing regulatory guidance, Boeing expects new specific compliance requirements from Section 941 of the National Defense Authorization Act for 2013 to be enacted within the year, which will cause additional reporting requirements for Boeing's Department of Defense contracted programs.

9. What organizational critical assets are interdependent upon other critical physical and information infrastructures, including telecommunications, energy, financial services, water, and transportation sectors?

- Business operations are dependent on telecommunications, energy, financial services, water, and transportation

- We have experienced cyber-attacks originating from compromised hosts in the networks of our peers, our customers (e.g., compromised US Air Force assets), our subsidiaries, and our supply chain. We are serviced by several ISPs. We try to encrypt our data going that is conveyed across ISP resources. Like other industries we have dependencies upon local electric power (we have electrical backups but they can't run indefinitely), water, and local transportation systems.

- Boeing relies on a global supply chain for Just In Time (JIT) manufacturing. Disruption to the global transportation systems would have an adverse effect to our critical businesses.

10. What performance goals do organizations adopt to ensure their ability to provide essential services while managing cybersecurity risk?

- We have mature, well-articulated disaster recovery, backup, and reconstitution plans and processes. We are moving our major data centers to environments having minimal earthquake, tornado, volcano, and other "force of nature" risk. These sites also are close to major electrical generation capabilities.

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?

- Boeing has filed over 130 (??) Incident Collection Form inputs to the Department of Defense Chief Information Office DIB Cybersecurity/Information Assurance Program since formally joining the program as a signatory of the Framework Agreement in March 2008.

- Elements disclosed to OSD and our DIB Cybersecurity Information Security Exchange Partners (DCISE - now numbering 74 companies) typically include; Time of Incident; Personal and Corporate Redacted Details on the Sender(s) and Recipient(s), C2, use of ports, Subject Lines, Copies of Malicious URL or Documents, MD5 associated hashes, and some idea of what files are dropped and where they are placed in directories; as potential indicators of advanced persistent threat tactics, techniques, and procedures for the benefit of the government and our DIB Partners. More recently actual copies of malware may be dropped as well as part of the DCISE reporting process.

- In terms of other regulatory bodies, Boeing is not as far along with in reporting requirements from the Federal Aviation Administration and Transportation Security Administration, and they do not yet have a portal for reporting neither standardized reports nor an ability to take in malware samples.

12. What role(s) do or should national/international standards and organizations that develop national/ international standards play in critical infrastructure cybersecurity conformity assessment?

- Security standards are very important to enable us to create interoperable cyber defense controls.
- Boeing's Aviation Cybersecurity compliance must also consider regulatory standards and reporting processes enacted by the International Civil Aviation Organization, in addition to FAA and TSA standards.

Questions Relating to Existing Frameworks from the RFI

1. What additional approaches already exist?

- ISO 27001 certification of an Information Security Management System
- ISO 10181-1, 10181-3
- X/Open Distributed Security Framework, The Open Group
- Framework for Secure Collaboration-Oriented Architectures, The Jericho Forum, Open Group, 2012
- And of course NIST Special Publication 800-53 (We have refrained from listing the many useful NIST publications in this document because we figure you are well aware of them.)

2. Which of these approaches apply across sectors?

- All of those listed above are sector independent

3. Which organizations use these approaches?

4. What, if any, are the limitations of using such approaches?

- An ISO 27001 certification is an evaluation of the information security management system in relation to the ISO 27002 control framework. It is not an evaluation of risk or the effectiveness of controls. The related ISO27005 provides further detail on risk management, although does not provide a risk analysis method.5. What, if any, modifications could make these approaches more useful?

5. What, if any, modifications could make these approaches more useful?

- Many regulatory and other frameworks concentrate on defining controls, apparently risk-based, for compliance measurement. Some “risk” reports from these compliance measurements are at best a subjectively prioritized compliance status. A more useful approach is to use controls frameworks to categorize local risk-based cybersecurity policy, employing analytical risk analysis based on the Open Group FAIR standard.

6. How do these approaches take into account sector-specific needs?

- Each sector likely has a common set of asset types and related threat actors used in their risk analyses. The risk analysis can benefit from sharing threat intelligence and incident experience.

7. When using an existing framework, should there be a related sector-specific standards development process or voluntary program?

- Enterprises each implement a unique system of security solutions, aligned to their security standards. A neutral international framework (e.g., ISO 27002) is beneficial for communicating control effectiveness between companies (e.g. evaluating supply chain security).

8. What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?

- They can provide relevant use cases to ensure that any general purpose framework meets their needs.

9. What other outreach efforts would be helpful?

- The internet is global and secret threats often cross nation state boundaries. Outreach to international security or standards organizations, other governments with cybersecurity programs, and global political entities (such as the OECD) should be considered.

Questions Relating to Existing Practices from the RFI

1. Are these practices widely used throughout critical infrastructure and industry?

- ISO 27001 certification is not widespread; it is difficult to assess the use of the ISO 27002 control framework. FAIR is relatively new, with early adopters in various industries.
- The US military has devised and codified very helpful Operational Security policies and procedures. It would be helpful if NIST could identity equivalent sets of recommended OPSEC policies and procedures for industry.

2. How do these practices relate to existing international standards and practices?

- The ISO 27001 Information Security Management System provides a model for a corporation's security governance process. ISO 27002 controls can be mapped to a corporation's security policies.

3. Which of these practices do commenters see as being the most critical for the secure operation of critical infrastructure?

4. Are some of these practices not applicable for business or mission needs within particular sectors?

5. Which of these practices pose the most significant implementation challenge?

- The urgency of detecting, responding and preventing attacks can out prioritize the good hygiene of implementing and operating a security management system.

6. How are standards or guidelines utilized by organizations in the implementation of these practices?

- Security policy establishes the authority and responsibility for an organization to implement a security program, including specifying the security controls that must be implemented for a reasonable risk level.

7. Do organizations have a methodology in place for the proper allocation of business resources to invest in, create, and maintain IT standards?

- One key objective of the security management system, and specifically risk analysis, is to prioritize security control requirements considering both risk reduction and implementation cost.

8. Do organizations have a formal escalation process to address cybersecurity risks that suddenly increase in severity?

- Yes*, both an escalation process for countering attacks and threats and a notification process to alert management* and executives.

9. What risks to privacy and civil liberties do commenters perceive in the application of these practices?

10. What are the international implications of this Framework on your global business or in policymaking in other countries?

- ISO 2700x frameworks are particularly appropriate due to their international nature.

11. How should any risks to privacy and civil liberties be managed?

- We have an executive level Global Privacy Office that in turn has an advisory board with cords organizational representation. Development of new cybersecurity controls is coordinated with this office.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Taxonomy Introduction

In order to manage and assess their effectiveness, an enterprise needs to organize their security services around a framework or taxonomy. While some answers appear above, the bulk of our answers are placed below in a framework. This framework is divided into two sections. The first section: *Governance* covers risk management, compliance, policies and user education. This is included primarily to provide additional detail to some of the more general questions responded to above.

The second, longer section: *Technical Services* covers information protection, applications, platforms, access control, intelligence gathering, and resilience. This is a technology and service based framework for organizing an enterprise's cybersecurity capability. The establishment of such a framework is itself a best practice. No existing standard or taxonomy covers this completely but relevant parts of NIST Special Publication 800-53, ISO 2700X and the Open Group's XDSF (X/Open Distributed Security Framework), APKI (Architecture for a Public Key Infrastructure), and OISM3 (Open Information Security Management Maturity Model) cover parts.

1. **Governance: Risk, Policy, Compliance & Education -** Communicates and enforces a set of defined controls which serve as a means of protecting systems against unauthorized access, use, disclosure, disruption, modification, inspection or destruction
   Best Practice - Start with governance… end with governance. Ensure a strong governance process exists before initiating a project or initiative.
   Best Practice - Ensure roles, responsibilities, accountabilities, and authorities are defined before initiating a project or initiative.
   Best Practice - Documentation should be the result of the processes we follow or the work we do. We say what we do… we do what we say… and we have document to prove it.
   Best Practice - Business processes, not technology, sales pitches, nor fads drive solutions

1.1. Risk Management - Develops and executes techniques to properly identify, articulate, assess, mitigate and report on information risk

Best Practice – Organizations should use a risk management process for balancing business needs and opportunities against the set of security services necessary to secure the enterprise from consequences of business decisions.

Best Practice – Organizations should use a standard taxonomy and set of definitions for describing risk. We have found that the Factor Analysis for Information Risk (FAIR) standard from The Open Group to be useful for this.

Best Practice - Manage risk proactively to minimize loss and capitalize on new business opportunities.

Best Practice - Base risk analysis on empirical evidence and methods rather than subjective input, it's best to use a formal methodology, such as FAIR, to organize risk components.

Practice Gap – Risk Taxonomies and risk management processes must be normalized and standardized in order to support collaboration among the various organizations supporting different components or aspects of a critical infrastructure. Risk needs to be addressed across the critical infrastructure and not compartmentalized based on arbitrary organizational alignment.

1.1.1. Security Policy Development - Creates a set of defined controls which serve as a means of protecting systems against unauthorized access, use, disclosure, disruption, modification, inspection or destruction

Best Practice – Organizations should use security policy to provide current, authoritative direction on a great depth and breadth of controls. This can result in an incomprehensible volume of policy requirements. In order to prevent overwhelming the end user, the cumulative body of policy must be filtered to only those pertinent to the user's needs. Key characteristics:

- Policy is attainable, enforceable and measurable
- Policy can be expressed in digital format (XACML) for access control over electronic resources
- The policy management system must be simple, dynamic, scalable, integrated and informative
- Policy is informed by risk and supports business needs
- Policy is related to regulations and control standards

1.1.2. Policy and Regulatory Compliance - Establishes, collects and reports metrics that can be used to track adherence to the recommended security controls

Best Practice – Organizations should measure the effectiveness of controls to allow managers and staff to determine how well controls achieve planned control objectives.

Compliance management is founded on the identified accountability for an individual system's compliance. The scope and frequency of measurement should be sufficient to provide confidence in the reported status of security controls. Key characteristics:

- Compliance is assessed for all controls within scope
- Compliance monitoring is facilitated by automating and centralizing event monitoring and reporting
- Corrective actions track accountability to closure
- Broad authorized visibility is provided on compliance status
- Compliance influences changes to policy
- Ensure policy is definitive (unambiguous), current (appropriate for the times), and tailorable
- Include rationale with policy requirements
- Document criteria for measuring compliance to policy in coordination with policy enforcement stakeholders
- Record the relationships between policy and industry or governmental regulations (e.g., ISO controls)
- Trigger policy change based on change initiators (business, incidents, compliance data, regulation, risk analysis)

Resource - The Unified Compliance Framework (UCF) is a tool for tracing relationships among multiple regulatory compliance frameworks applicable to a corporation.

Best Practice - Check information systems regularly for compliance with security implementation standards; systems should automatically report compliance where possible.

Best Practice - Assign corrective actions to the appropriate individual to resolve and track the resolution to closure.

Best Practice - Provide visibility regarding the status of corrective actions to achieve desired outcomes; provide summary and drill down view of selected compliance items.

Best Practice - Ensure systemic issues identified using trend and root cause analyses are addressed through closed loop corrective action.

Best Practice – Information Sharing: (details below)

1.1.2.1 As a voluntary participant in the OSD CIO Defense Industrial Base Cybersecurity/Information Assurance Program and its existing Framework Agreement and Interim Federal Rule, Boeing actively shares cybersecurity incident information with the Department of Defense and its Defense Industrial Base Partners. This is in addition to any contractual obligations to share information with the government on cybersecurity related incidents and/or report any damage or leaks of government technology or other critical programmatic information in terms of impacts to Department of Defense Programs.

1.1.2.2 Additionally, the Security and Exchange Commission's Corporation Finance Disclosure Guidance dated October 13, 2011 requires registrants to *"address cybersecurity risks and cyber incidents in their Management's Discussion and Analysis (MD&A) section if the costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition"... "If one or more cyber incidents materially affect a registrant's products, services, relationships with customers or suppliers, or competitive conditions, the registrant should provide disclosure in the registrant's 'Description of Business.'"*

1.1.2.3 In addition to existing regulatory guidance, Boeing expects new specific compliance requirements from Section 941 of the National Defense Authorization Act for 2013 to be enacted within the year, which will cause additional reporting requirements for Boeing's Department of Defense contracted programs. The following details some of the key impacts to be expected in the updated National Defense Authorization Act for 2013:

1.1.2.4.1 PROCEDURES FOR REPORTING PENETRATIONS.—The Secretary of Defense shall establish procedures that require each cleared defense contractor to report to a component of the Department of Defense designated by the Secretary for purposes of such procedures when a network or information system of such contractor that meets the criteria established pursuant to subsection (b) is successfully penetrated.

1.1.2.4.2 PROCEDURE REQUIREMENTS —The procedures established pursuant to subsection (a) shall require each cleared defense contractor to rapidly report to a component of the Department of Defense designated pursuant to subsection (a) of each successful penetration of the network or information systems of such contractor that meet the criteria established pursuant to subsection. Each such report shall include the following:

1.1.2.4.2.1 (A) A description of the technique or method used in such penetration.

1.1.2.4.2.2 (B) A sample of the malicious software, if discovered and isolated by the contractor, involved in such penetration.

1.1.2.4.2.3 (C) A summary of information created by or for the Department in connection with any Department program that has been potentially compromised due to such penetration.

1.1.2.4.3 ACCESS TO EQUIPMENT AND INFORMATION BY DEPARTMENT OF DEFENSE PERSONNEL.—The procedures established pursuant to subsection (a) shall

1.1.2.4.3.1 (A) include mechanisms for Department of Defense personnel to, upon request, obtain access to equipment or information of a cleared defense contractor necessary to conduct forensic analysis in addition to any analysis conducted by such contractor

1.1.2.4.3.2 (B) provide that a cleared defense contractor is only required to provide access to equipment or information as described in subparagraph (A) to determine whether information created by or for the Department in connection with any Department program was successfully exfiltrated from a network or information system of such contractor and, if so, what information was exfiltrated; and

1.1.2.4.3.3 (C) provide for the reasonable protection of trade secrets, commercial or financial information, and information that can be used to identify a specific person.

1.1.3. Partner and 3rd Party Integration - Ensures that all personnel who leverage information are aware of their security control obligations as they relate to the access, use, disclosure, disruption, modification, inspection or destruction of the information, Compliance measured by collecting electronic records from partners and third parties.

Best Practice - Conduct risk and compliance reviews to ensure appropriate administrative and technical controls are in place before engaging partners or 3rd parties.

Best Practice - Use partners and 3rd parties that have been thoroughly vetted and pre-approved.

Best Practice - Vet partners and 3rd party employees thoroughly.

Best Practice - Restrict partners and 3rd parties to low risk countries for high risk statement of work.

Best Practice - Require partners and 3rd party companies to sign contractual agreements to provide recourse in the event of data loss or security incident.

Best Practice - Require partners and 3rd party employees to sign contractual agreements to provide recourse in the event of data loss or security incident.

Best Practice - Ensure partners report use of 3rd parties to complete assigned statement of work.

Best Practice - Require partners and 3rd parties to report computing security incidents or attacks.

Best Practice - Complete site assessments of partners and 3rd parties.

Best Practice - Track & periodically review the activities of partners and 3rd party employees.

Best Practice - Complete thorough background checks for partners and 3rd party employees.

1.1.4. End User Education – Periodic training, reminders, internal documents and media to update and remind all employees of best security practices

Best Practice - Knowledge is actively transferred throughout a product/service lifespan to help reduce single points of failure.

Best Practice - Customers are educated so they can become a proactive part of securing the enterprise.

Best Practice - Provide training in tool use and secure coding

Recommendation - Boeing supports DHS and NIST in establishing the National Initiative for Cybersecurity Education (NICE), but we believe the individual components lack an interconnection and application that could be even more valuable in increasing comprehension and ability to apply these skills against ever adaptive and evolving adversaries. These components are:

Component 1: National Cybersecurity Awareness

The National Cybersecurity Awareness Component is being led by the Department of Homeland Security. To boost national cybersecurity awareness, DHS will use public service campaigns to promote cybersecurity and responsible use of the Internet, and make cybersecurity a popular educational and career pursuit for older students.

As part of awareness, Boeing supports the National Cybersecurity Alliance "*Stop. Think. Connect*." campaign as a national public awareness effort and best practice to guide the nation to a higher level of Internet safety by challenging the American public to be more vigilant about practicing good "cyber hygiene" to help Americans increase their safety and security online.

Component 2: Formal Cybersecurity Education

Boeing supports Department of Education and the National Science Foundation (NSF) efforts to bolster formal cybersecurity education programs from kindergarten through 12th grade, higher education and vocational programs; and its focus on science, technology, engineering and math disciplines to improve employee skills for the private sector and government.

One area of formal cybersecurity education would be to emphasize strategic partnerships between industry and higher education where not only education, but also internships are available as practicum options. Boeing and many other industries have been studying how many youth choose Science, Technology, Engineering, and Math (STEM) related fields as they enter college. In 2011, Boeing invested approximately $50 million toward external education programs, with more than $23.7 million directed towards science, technology, engineering and math (STEM) programs.

Boeing IT is expanding its involvement in STEM. Our program touches all disciplines but focuses on IT. It is an effort to provide Boeing IT STEM specific curriculum and/or support other Boeing affiliated local youth engagement opportunities.

Boeing regularly finds that incoming graduates of technical schools lack sufficient training in the security aspects of their disciplines. For example, application developers often graduate without any formal training in secure coding methods or threat modeling. Higher educational programs could improve their integration of security principles into their existing curriculums.

Component 3: Cybersecurity Workforce Structure

Boeing supports the NIST objectives of establishing a Cybersecurity Workforce Structure Strategy and its focus on talent and effective management of cybersecurity professionals. By reaching out to Universities and establishing Internships and practical work for our needed cybersecurity skills, these internships allow Industry to evaluate the professionalization of its future workforce, and to identify the best and brightest skilled interns for recruitment and retention, and also train these individual on our corporate best practices and expectations.

Component 4: Cybersecurity Workforce Training and Professional Development
Boeing supports the NIST Cybersecurity Workforce Training and Professional Development initiative to intensify training and professional development programs, but questions why it would be limited to the Federal Workforce alone to encompass the training and response needs of a truly integrated Public – Private Partnership.

***Recommendation* -** In addition to the 4 primary components of the existing NIST National Initiative for Cybersecurity Education (NICE), Boeing considers there may be a 5th Component that would be useful to consider going forward and could also serve to unify the effectiveness of all 4 of the primary components.

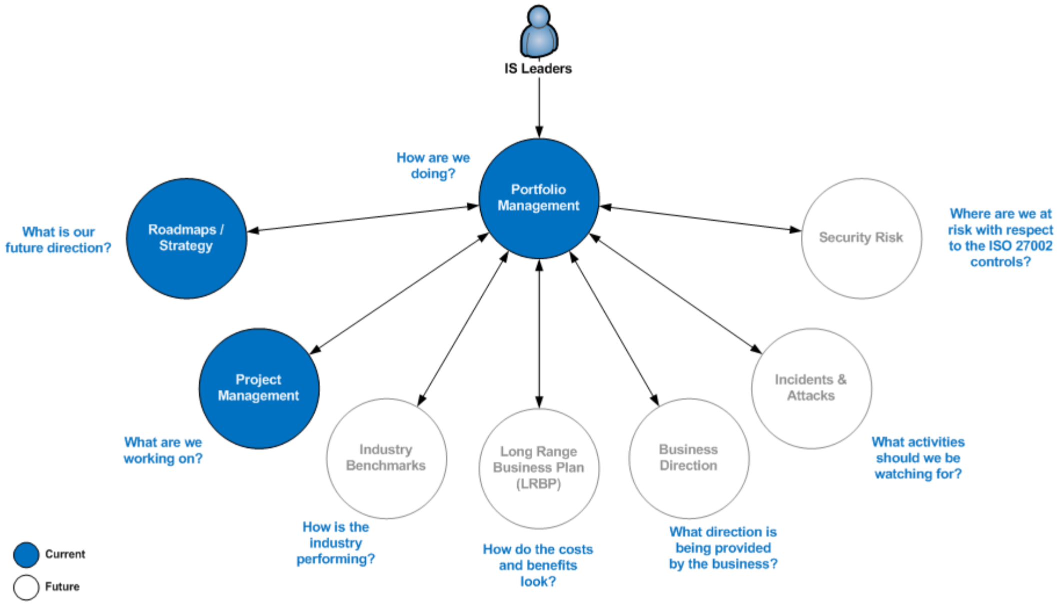
Component 5: Immersive Training and Education

Boeing is interested in the additional value cybersecurity in having a workforce that is capable of handling constantly adaptive and creative adversaries that by nature continue to evolve to meet their objectives. Experiential learning is a process through which students develop knowledge, skills, and values from direct experiences outside a traditional academic setting. Immersive environments help students retain more information through personal experience and speed up their learning.

In application a cybersecurity immersive education and training strategy would augment the 4 existing NIST National Initiative for Cybersecurity Education (NICE) components with realistic and interactive immersion and gaming methods.

1.2. Service & Portfolio Management - Assembles major goals and objectives which support the business strategy into a defined set of initiatives and prioritizes the efforts associated with the execution of the various initiatives

Best Practice - Consider multiple factors when prioritizing work (e.g., risk mitigation, strategic alignment, industry benchmarks, business plans, incidents, attacks, security risk).
Best Practice - Conduct regular management and technical gated reviews to ensure projects are on track.


IS Leaders
How are we doing?
Portfolio Management
What is our future direction?
Roadmaps / Strategy
Security Risk
Where are we at risk with respect to the ISO 27002 controls?
Project Management
What are we working on?
Industry Benchmarks
How is the industry performing?
Long Range Business Plan (LRBP)
How do the costs and benefits look?
Business Direction
What direction is being provided by the business?
Incidents & Attacks
What activities should we be watching for?
● Current
○ Future

1.2.1. Strategy & Roadmaps - Document the strategies, tactics, transition plans, and various projects as they related to accomplishing specific Information Security specific goals

Best Practice - Assign the responsibility of completing strategies and roadmaps to a sponsor who understands the need for future direction and will ensure the work is started and properly maintained.

Best Practice - Ensure that the strategy addresses people, governance, process, and technology.

Best Practice - Use the framework to document strategic direction, ensure alignment with strategic direction, directs solution architecture and design, and improves solution delivery through the use of patterns, decision frameworks, and reusable components.

Best Practice - Understand business drivers; the needs and trends within the business that will influence strategic direction.

Best Practice - Document and enforce principles; lessons learned and other general guidance which ensures that all projects and initiatives follow a set of common norms.

Best Practice - Depict a reference model; a taxonomy for organizing strategies; the taxonomy can influence the organization structure but the organization structure should not influence the taxonomy.

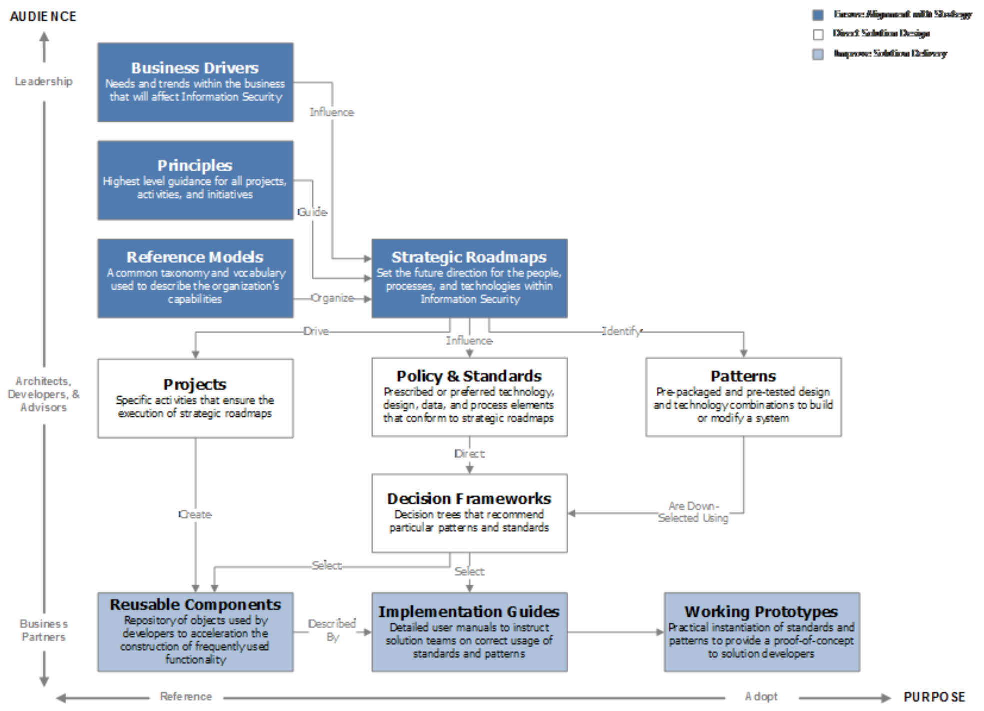
Best Practice - Document strategic roadmaps; strategic direction at two basic levels: (1) long term direction that is implementation agnostic and (2) mid to short term direction that is implementation specific.

Best Practice - Identify projects, policies, standards and patterns; these do the dirty work of driving alignment to the strategic direction.

Best Practice - Produce reusable components and working prototypes; eliminates need to reinvent solutions over and over again.

Best Practice - Review strategy and roadmap materials periodically to ensure they are kept current.

Best Practice - Regularly communicate strategy and roadmaps to the organization and ensure each individual understands his/her responsibilities in fulfilling the stated direction.



AUDIENCE
Leadership
Architects, Developers, & Advisors
Business Partners
Ensure Alignment with Strategy
Direct Solution Design
Improve Solution Delivery
Business Drivers
Needs and trends within the business that will affect Information Security
Principles
Highest level guidance for all projects, activities, and initiatives
Reference Models
A common taxonomy and vocabulary used to describe the organization's capabilities
Influence
Guide
Organize
Strategic Roadmaps
Set the future direction for the people, processes, and technologies within Information Security
Drive
Influence
Identify
Projects
Specific activities that ensure the execution of strategic roadmaps
Policy & Standards
Prescribed or preferred technology, design, data, and process elements that conform to strategic roadmaps
Patterns
Pre-packaged and pre-tested design and technology combinations to build or modify a system
Direct
Decision Frameworks
Decision trees that recommend particular patterns and standards
Are Down-Selected Using
Create
Select
Select
Reusable Components
Repository of objects used by developers to acceleration the construction of frequently used functionality
Described By
Implementation Guides
Detailed user manuals to instruct solution teams on correct usage of standards and patterns
Working Prototypes
Practical instantiation of standards and patterns to provide a proof-of-concept to solution developers
Reference
Adopt
PURPOSE

1.2.2. Project Management - Plans, organizes, secures, manages, leads, and controls resources to complete a temporary endeavor (project) undertaken to meet specific goals, strategies, and tactics.

Best Practice – Use a good software development process that includes gates or reviews when developing software. We use a set of processes called Macroscope, currently owned by Fujitsu.

Best Practice – Early in a project's lifecycle, there should be a Security Design Review (SDR). The function of the SDR is to determine that the proposed architecture, design and service set of the project complies does not introduce unacceptable security risk to the enterprise. This review should be early enough in the project's lifecycle to allow for design changes.

Best Practice - Start with business requirements first, even if the business has a proposed solution. Identify security risks for the business problem and provide solution alternatives.

Best Practice - Remember Eisenhower's statement… "Plans are nothing; planning is everything"; be adaptable because change is the only constant.

Best Practice - Ensure all projects align to strategic direction.

Best Practice - Ensure project plans account for all work currently underway, not just the specific project that is being considered.

Best Practice - Ensure project schedules are properly level-loaded.

Best Practice - Analyze costs/benefits and return on investment throughout the project lifecycle.

Best Practice - Cancel projects that are not adding value or aligning to strategic direction.

Best Practice - Plan adequate time for maintenance and operational tasks (e.g., upgrades, compliance tasks); these activities account for 80%-90% of a product's lifetime.

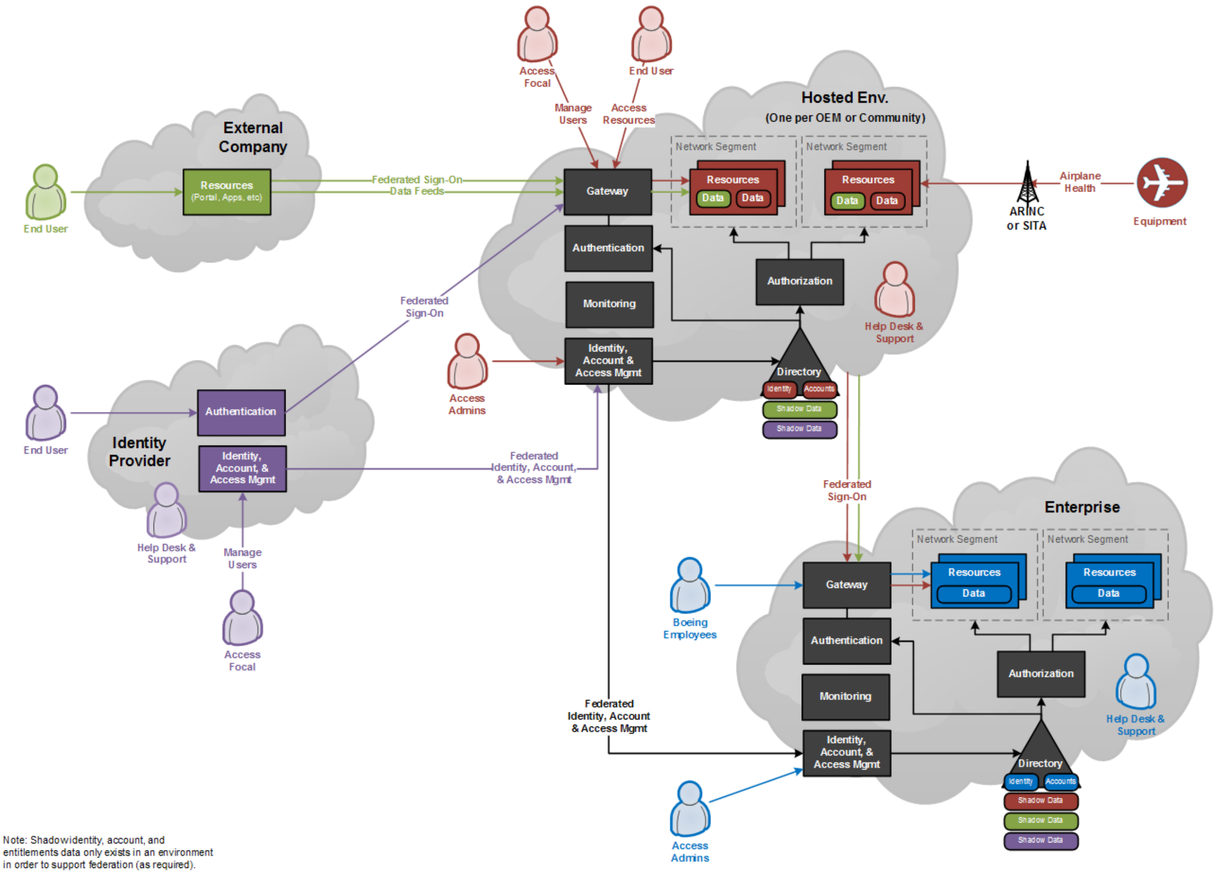
1.2.3. Product Lifecycle Management - Provides a means of identifying and replacing obsolete technologies with emerging technologies while also providing a way of integrating these emerging technologies with existing technologies

Best Practice- Ensure products have a clearly defined scope and purpose; keep the system bounded to the scope and purpose.
Best Practice - Sub-Divide a multi-function product into several single-function products to promote proper design and facilitate reuse.
Best Practice - Identify a target retirement date at the beginning of a products lifecycle to ensure products do not live on unnecessarily; the retirement date may change but there should be a sound exit strategy in place well in advance of product retirement.

1.2.4. Patch Management - Executes a strategy which enables timely updates to systems as a means of maximizing system stability, security and performance

Best Practice - Perform system upgrades and patches separately from changing existing or introducing new functionality; if multiple things change it will it will be harder to identify the root cause when something fails.
Best Practice - Perform system upgrades and patches on a regular basis; stay within 1 major version of a product

2. Technical Services - The collection of technical controls and security services that protect enterprise data, communication, platform and other IT components from compromise while preserving their availability for legitimate users



Note: Shadowidentity, account, and entitlements data only exists in an environment in order to support federation (as required).

2.1. Data Protection - Provides the appropriate controls to ensure data (e.g., structured database, unstructured files) is adequately secured and protected.

Best Practice - Protection should be consistent throughout the lifecycle of the data. Typically, this includes creation, modification, distribution, archive, and destruction. The point is that there should be consistent protection applied to the data at each of these stages, or until the data is securely destroyed. The entity that owns or manages the data may make an explicit change to its protection profile, but this capability to provide consistency should be the default.

Best Practice - Protection should be consistent across space as well as time. That is, the protection applied to the data should be the same regardless of its location or environment. This means that there is consistency regardless of where the data is stored – on a computer, in a database (RDBMS), attached to an email, in transit through a VPN, present on a smart phone, etc. Information about the geographical location of data is also an important criterion for determining access control for location sensitive data – such as export controlled information.

Best Practice - Data protection systems should support both structured and unstructured data. Examples of structured data include drawings managed by computer aided design systems (CATIA, DELMIA, ENOVIA, etc.), data held in relational database management systems (RDBMS), data managed by complex applications (email, ERP, SharePoint, WebEx, etc.), and data held in sophisticated storage management systems (EMC Documentum). Examples of unstructured data include office files (documents, presentation materials, spreadsheets, etc.) as well as text files, configuration files, and other discrete digital objects. Unstructured data files are commonly found on file shares, webservers, document repositories, and even laptops and mobile devices.

Best Practice - Data protection systems should also support continuous or network packet based data such as voice, video, etc. In order to effectively leverage data, protection must be applied at the data layer itself. While protection at the lower layers (application, operating system, network, and physical storage) tends to be cheaper and more manageable the deeper you go, the flexibility of e-commerce diminishes, since there is less and less interoperability at the same time. The scope of protection tends to expand as well.

Best Practice - Data protection systems should also be based on interoperable standards, such as XACML. This facilitates consistent enforcement of policies across disparate platforms and applications. Furthermore, data protection systems should be integrated (by means of XACML) with application and network layer protection systems.

Best Practice - Since protection will be applied to the data by an application running on an operating system that should not be trusted, there should be a separate, strong authentication mechanism when the data is protected or accessed that is independent of the operating system. Ideally this would have an option to use a TCG TPM (Trusted Platform Module), smart card, or other secure cryptographic device as a trust root.

Best Practice - Protect our most valuable asset --the data-- by moving the enforcement mechanisms as close to the data as possible. Protections, if at all possible, should move with the data and be there regardless of the environment.

Best Practice – Enforce the principle of Least Privilege for data access. Restrict privileges to only those that are essential to complete the assigned Statement of Work. Restrict access to shared databases that store data other than what is needed to complete the assigned Statement of Work. Grant access to production data only if this requires it

Best Practice - Enforce the principle of Defense in Depth for data: Harden/remove database links to prevent transitive access. Ensure adequate separation between data that is allowed for the Statement of Work and data that is not allowed. Ensure production data only exists in production environments. Sanitize data in non-production environments

Best Practice - Ensure backups of production data are encrypted.

Best Practice- Ensure that at least one copy of the backup is kept on offline media.

Best Practice - Catalog and label data to enable mandatory access control to data.

Practice Gap – Consistent enforcement of data access decisions across a critical infrastructure supported by multiple organizations must be based on a common information classification taxonomy, access policy definitions, and standardized identity, authentication and authorization criteria data. This implies a certain degree of commonality in data modeling, policy development, and identity and access governance. Such classification, policy and decision data must adhere to a common set of standards across the supporting organizations or consistent data protection cannot be achieved throughout its lifecycle or across the field of its use.

2.1.1. Information Assessments - Locates and secures sensitive information contained within various data storage systems
Best Practice - At least some Assessments should happen in real-time without any human interaction. The state of data should be continuously monitored and aberrations should automatically be detected and reported.

2.1.2. Labeling - Analyze data for appropriate regulatory or contractual classification and apply resource metadata (e.g., visible, meta-tags, a.k.a. “tagging” or “marking”; either through manual or automated means) to facilitate evaluation by XACML-based access control systems. This can prevent misuse or inappropriate distribution either through manual or automated means and control information exchange in a collaborative environment.
Best Practice – Organizations should use standard taxonomies for constructing labels. The OASIS labeling standard is recommended.
Best Practice – Labels should be created automatically when data is created. There should, however, be an override that the data owner can use to change the labels.

2.1.3. Signing - Provides non-repudiation of the author and guarantees that the data and resource metadata has not been altered or corrupted since it was signed by use of a cryptographic hash

Best Practice – Require signature prior to transmission of data to ensure integrity. Require signature for data that is critical to the functioning of systems where high reliability is required.
Best Practice- Retain archives of public keys to enable the verification of signatures over the long term.

2.1.4. Encryption - Transforms data at rest using cryptography to produce ciphertext which is not human readable and which may not (for appropriate reasons) be decipherable. Encryption types and actions should be governed by digital policy, interoperable, and capable of supporting multiple platforms and applications.
Best Practice - Require encryption of highly sensitive data prior to transmission or storage.
Best Practice = Ensure processes that operate on highly sensitive data do not allow other processes to view said data in cleartext.
Best Practice - Use only known, trusted algorithms that meet minimum strength requirements.
Best Practice – Provide adequate protection for private keys. This include both technical solutions and user education.

2.1.5. Digital Rights Management - Limits or inhibits the use of digital content that is not desired or intended by the content provider

Best Practice - Data protection systems should be able to distinguish discrete activities or actions applied to the data and enforce permissions based on those actions. They should separately control the user's ability to create, modify, delete, read, infer from, distribute, convert formats, archive, manipulate, etc. Data protection systems must also perform fine-grained access control based on a rich set of attributes beyond the typical identity and action attributes and evaluate the context of the access request. For example, environmental factors, such as location and time must be considered. They should also support the use of authentication, pseudonymity, and anonymity, and access by individuals or groups as required. The OASIS XACML standard is the most applicable to protecting data. XACML policies can govern (through use of the "Obligations" element) how and when encryption is applied to resources. However, there is a need for a standard encrypted container or protection mechanism and accompanying API to facilitate interoperable rights management protection technology.

2.1.6. Data Loss Prevention (DLP) - Detects potential data breach incidents in timely manner and prevent them by monitoring data while in-use (endpoint actions), in-motion (network traffic), and at-rest (data storage). DLP tools should be configurable by utilizing XACML policies. Moreover, DLP tools should be able to scan for and apply standardized metadata tags. For examples, see http://docs.oasis-open.org/xacml/3.0/ipc/v1.0/cs02/xacml-3.0-ipc-v1.0-cs02-en.doc and http://docs.oasis-open.org/xacml/3.0/ec-us/v1.0/cs02/xacml-3.0-ec-us-v1.0-cs02.doc.

Best Practice - Integrate DLP with security incident and event monitoring (SIEM) systems to correlate server, network, and endpoint device events

2.2. Software Security – Ensure applications, operating systems, processes and software components adhere to security principles and practices throughout the development lifecycle.

Best Practice – As a general rule, applications and particularly security applications are easier to analyze for good security properties if they are designed for a specific purpose. Multipurpose applications run the risk of significantly increasing the attack surface and encouraging side channel attacks between different functions – these are hard to analyzed and defend against. While there will always be complex, multi-use applications (and the operating system is the ultimate example) when writing specific applications, consideration should be given for encouraging as narrow a scope as possible. Smaller applications are easier to test and secure, and collections of smaller applications that use open standards to coordinate provide better flexibility and scalability across an enterprise and are easier to integrate between enterprises.

Best Practice – It should be possible to replace one technical solution with another without requiring applications to re-plumb to the security services.

Best Practice - Protect solutions that serve as the foundation of other services by using security measures that are at least as strong as those of the consuming services.

Best Practice - Ensure all development organizations follow the same secure development lifecycle; regardless of their position within the enterprise organization structure.

2.2.1. Secure Design & Development - Ensures IT products (people, processes, and technology) are built and maintained with security in mind

2.2.1.1. Secure Development Lifecycle - Identifies the processes and provides the means by which IT products must be designed, built, tested, and maintained to uphold security principles

Best Practice - Integrate security into the overall solution by addressing security considerations from the beginning of the development lifecycle.

Best Practice – Use professional software development techniques: Use CERT standards for development, they have document lots of good security development practices, Use source code control systems, automate builds, perform daily builds, use a bug database and fix bugs before adding functionality as bugs can often be exploited. Have a separate test team and train them in exploiting security vulnerabilities. Keep developers trained in best practices and new technologies, including security. Maintain/update your code versions and libraries – this is as important as patching your OSs.

Best Practice – Early in a project's lifecycle, there should be a Software Design Review. The function of the review is to determine that the proposed architecture and design of the software complies does not introduce unacceptable security risk to the enterprise. This review should be early enough in the software lifecycle to allow for design changes.

2.2.1.2. Threat Modeling - Identifies the processes and provides the means by which IT products are scrutinized in order to identity threats to security, proposed mitigations to those threats, and clearly identify any unmitigated threats as product vulnerabilities.

Best Practice – The Threat Modeling (TM) document should be updated continuously through the system development. Preliminary TM delivered during Initial Design Review. Detailed TM complete for Technical Design Review.

Best Practice – Threat Modeling should be updated with Residual Risk after mitigation is applied. This provides an accurate representation to Program Manager of the system security risk.

Best Practice - Implement threat modeling as a continuous aspect of the product; threat modeling is an ongoing exercise because the product changes or the environment changes.

Best Practice - Threat Assessments (rather than simply threat modeling) includes four major steps: (1) modeling of the solution, (2) collection of important factual details, (3) identification of vulnerabilities, and (4) assessment of possible mitigations.

Best Practice - Treat threat assessments as you would any other type of highly sensitive data since the threat assessment provides a map of attack vectors for malicious individuals to exploit.

Best Practice - Create models that depict all objects (e.g., servers, process steps, actors, and software components) and the interactions between them; provide guidance which focuses the attention on depicting all objects and the collaboration between them rather than mandating a specific diagramming format.

Best Practice - Collect important factual details about all entities in the model; provide guidance which focuses attention on identifying what each entity "has or does" and how each of those items is secured; ask questions like "what data is used by the process and how is the data protected" rather than questions like "is data used by the process encrypted?" since the former question will require an in-depth response where the later question requires a simple yes/no answer.

Best Practice - Identify all vulnerabilities for each entity in the model; be thorough when describing the vulnerability; describe how the vulnerability can be exploited; assess the impact of the vulnerability using objective rather than subjective means since different individuals accept risk differently; include vulnerabilities that have already been mitigated.

Best Practice - Identify all possible mitigations for a vulnerability; describe how the mitigation can be tested; identify to what degree it reduces the impact of the vulnerability

2.2.1.3. Application Assessments - Ensures applications are secured and protected from the threats identified as part of the threat model

Best Practice - Incorporate assessment findings into the development lifecycle to ensure vulnerabilities are addressed sooner in the development lifecycle.

2.2.1.4. Code Scanning - Ensures that code modules, procedures, and objects are free from known vulnerabilities (e.g., cross-site scripting, SQL injection)

Best Practice - Perform code scanning prior to the initial release of a solution, at regular intervals, or when major enhancements are made to a solution.

Best Practice – Code Scanning should be used. It is rapidly becoming a best practice and we have been requiring it internally for all new software projects for about a year. We are also requiring third parry attestation to positive results of code scanning for all vendors' products. There are some things to keep in mind when doing code scanning:

- One tool does not cover all types of languages or purposes of s/w – use the right tool. Use the scanning tool that has expertise in that language and type of application (for example a scanning tool that is great for java web apps may not be great at something else) Each individual tool has its limitations and so multiple tools should be used to provide the best overall coverage.

- Do not confuse scanning tools for developers as quality measurement for management. The results of these tools should be treated as advisory and not authoritative. Hence they should be managed in the same way as normal bugs and not abused by being used as a metric of goodness which might have the effect of discouraging the use of the tools.
- Different tools are useful at different stages in the development process. Source code analysis of individual modules tends to be more useful to developers as compare to a late stage binary analysis of entire programs.

Standards – there needs to be standards for code scanning that would include types of things to scan for, common reporting standards, etc. Vulnerabilities should be based on existing standards such as NIST SCPA and the emerging IETF SACM standards.

Best Practice – Supplement Scanning Tools - Have code reviews specific to security vulnerabilities (many are not caught by scanning tools). Train code reviewers in how to determine back doors (scanning tools do not find this).

Best Practice – Code scanning techniques should be reviewed regularly to ensure they are addressing current threats and utilizing the latest tools. Code scanning should be performed at least on a yearly basis or major functionality changes. Developers should incorporate tools into their normal work flow.

Practice Gap – Collaborative endeavors among organizations, especially in support of a critical infrastructure, depends on some assurance that the applications used have a common degree of code security. Typical current code scanning practices are based on specific organizational criteria, if they exist at all. Standard code security criteria need to be established and required minimum levels of code security need to be established various critical infrastructure support domains. The Open Web Application Security Project (OWASP) publishes its “Top Ten” criteria, which may be a good starting point. 3rd Party certification of code security may also be an approach to achieve common levels of code security assurance.

2.2.2. Application Protection - Provides the appropriate controls to ensure applications (e.g., web, thick client, mobile) used to access data and other resources is adequately secured and protected.

Best Practice – Security externalization. Applications should externalize authentication and authorization decisions rather than making those decisions themselves. Externalizing these decisions allows applications to use general purpose policy decision engines that can be deployed by an enterprise as a centralized security service. It also limits the amount of security relevant code that needs to be written, thus reducing the software attack surface. As an example, we have deployed (as part of a widely used web based single sign on service) a toolkit that gives an internal developer and API to make authentication call to. We have created a similar service for making real time authorization decisions (so far export and IPR) for CAD drawing elements. A third advantage is the disintermediation of the protection mechanisms from the application. We can change the authentication mechanisms (for example disallow passwords and require a smart card) without impacting the protected application. Relevant standards include LDAP for access to end user meta data, SAML for authentication assertions and XACML for authorization.

Best Practice - Develop, distribute, and publish reusable service modules for application protection (e.g. Authentication, Encryption Key Handling, Authorization, Web Services Security, etc.).

Best Practice - Ensure applications used to execute the Statement of Work have been scanned and findings mitigated.

Best Practice - Provide each administrator his/her own privileged account. Administration accounts that provide access to either large amounts of data or sensitive data should be protected using strong authentication.

Best Practice - Ensure applications use standard authentication mechanisms (e.g. Active Directory, Web Single Sign On).

Best Practice - Restrict privileges to only those that are essential to complete the assigned Statement of Work.

Best Practice – White list allowed applications – that is, use tools that prevent any applications that are not explicitly designated from running. Typically this tools can be used in a “block & ask” mode to make it easier to allow new applications to be easily added. The point is that the end user or administrator will have to accept the request and this prevents malware from automatically installing and running programs.

Practice Gap – Consistent enforcement of application access decisions across a critical infrastructure supported by multiple organizations must be based on a common sensitivity classification taxonomy, access policy definitions, and standardized identity, authentication and authorization criteria data. This implies a certain degree of commonality in application standards, policy development, and identity and access governance. Such classification, policy and decision data must adhere to a common set of standards across the supporting organizations or consistent data protection cannot be achieved throughout its lifecycle or across the field of its use.

2.2.2.1. **Firewalls & Isolation** - Enforces a boundary around the application code, configuration, and data to prevent tampering, unauthorized access, and data leakage
Best Practice – Application firewalls should be used to protect data flows and ensure that they are limited to their proper destinations.
Emerging Best Practice – Virtualization provides significantly stronger application protection than software based firewalls.
Best Practice - Use virtual machines to shrink attack surface. Codebase is measured in KBytes instead of Mbytes. This size is within reach of correctness proof capability. Separate VMs used for dedicated sub-OS functions. There should be a similar

structure for complex applications. Separate VMs for critical, normal, and high risk functions and applications.
Best Practice – Process and device driver sandboxing.
Best Practice – Dual SSL/HTTP network stacks—one stack for known domains based on a large white list and another stack for unknown domains.
Best Practice - Mandatory access control and trusted path implementation. See this paper: The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments, Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, Ruth C. Taylor, S. Jeff Turner, John F. Farrell; National Security Agency.
Best Practice – Dynamically block source IP's that are running network enumeration tools.
Best Practice - Use an application layer firewall to assure approved data flows are behaving as expected.
Best Practice - Require a security review of dual homed systems.

2.2.2.2. **Hardening** - Locks down an application in order to minimize the attack surface by disabling or removing unused, unnecessary, or risky components
Best Practice - Utilize virtual and hardware based sandboxing techniques to contain applications.
Best Practice – Turn off unnecessary services.
Potential Direction - Automatic restoration from a trusted source without interrupting users - this would be done after a certain amount of risk had been reached and could be implemented using multiple VMs that would switch back and forth.

2.2.2.3. **Signing** - Provides non-repudiation of the software author and guarantees that the code has not been altered or corrupted since it was signed by use of a cryptographic hash
Best Practice - Require COTS vendors, internal developers, partners, and 3rd party providers to digitally sign all software components.
Best Practice- Protect signing keys from misuse or copying. Even better, keep the private keys used for signing in an HSM.

2.2.2.4. **Web-Services Security** - Ensures the appropriate authentication, authorization, and cryptographic measures are taken to ensure communication with application web services (e.g., SOAP, REST)

2.2.3. Cloud Computing Security – Ensures that data is protected when cloud computing services are used
Best Practice – Review cloud providers and applications utilizing ISO 27002 control requirements and Cloud Security Alliance guidelines. Ensure that controls are aligned with internal governance control frameworks.

2.2.3.1. **Data Transmission and Data Security** – ensures that data is protected when being transmitted to and from cloud services. Managing data that is placed in cloud, identifying controls of data in the cloud as well as compensating controls that can be used to deal with the loss of physical control when moving data to the cloud.

Best Practice - Follow and protect data throughout the data security lifecycle i.e. in all 6 phases of data lifecycle, Create, store, use, share, and archive and destroy.
Best Practice - Secure data in transit as well at rest using encryption technologies (client/application encryption, or link/network encryption or proxy based encryption) and use storage with data dispersion.
Best Practice - Information classification and governance policies need to be clearly defined based on jurisdictional controls.
Best Practice - Define types of authentication and authorization needed for access to different data types.
Best Practice - Ownership and custodianship to be clearly identified for the information.
Best Practice - Detection and preventing migration to the cloud: Depending on policy certain data types may be restricted from moving into the cloud. Hence it is important to monitor large internal data migrations with DAM (Database Activity Monitoring and FAM (File Activity Monitoring)
Best Practice - Use URL filters and DLP tools in when migrating data to the cloud.

2.2.3.2. Portability and Interoperability – To avoid potential data and application loss, it's important to remain flexible when choosing a cloud environment.

Best Practice - Use Open standards for Virtualization e.g. OVF
Best Practice - Use Virtualization and abstraction layers to abstract form the physical hardware layer, it's important to understand the specific virtualization hooks that are used regardless of the format.
Best Practice - Frameworks: investigate API's to determine where differences lie and plan for changes necessary that may be required to applications when moving to a new provider.
Best Practice - Use open and published standard API's to ensure broadest support for interoperability between components and to facilitate migrating applications and data should there be a change in provider.
Best Practice - Applications should be able to interoperate in the cloud, hence the impact of outages on transactions should be identified before deploying them.
Best Practice - SLA's may be different across providers, these need to be taken into consideration when switching providers.
Best Practice - Platform architectures may be different when the provider is changed hence it's important to design applications or services that do not rely on one particular platform
Best Practice -Metadata is another key aspect which needs to be protected when migrating from one provider to another, the metadata files should be securely removed from the old provider for security reasons.

Best Practice - Understand how virtual machine images can be captured and ported to new cloud providers, who may use different virtualization technologies.

- Identify and eliminate (or at least document) any provider-specific extensions to the virtual machine environment. Understand what practices are in place to make sure appropriate deprovisioning of VM images occurs after an application is ported from the cloud provider. Understand the practices used for decommissioning of disks and storage devices. Understand hardware/platform based dependencies that need to be identified before migration of the application/data. Ask for access to system logs, traces, and access and billing records from the legacy cloud provider.

- Identify options to resume or extend service with the legacy cloud provider in part or in whole if new service proves to be inferior. Determine if there are any management-level functions, interfaces, or APIs being used that are incompatible with or unimplemented by the new provider.

2.2.3.3. Application Security: Control over physical security is substantially reduced in public cloud scenarios, potential incompatibility between vendors when services are migrated from one vendor to another. Protection of data and metadata throughout the development lifecycle. Hence follow secure development lifecycle.

IaaS, PaaS, and SaaS create different trust boundaries for the software development lifecycle; which must be accounted for during the development, testing, and production deployment of applications.

Best Practice - For IaaS, a key success factor is the presence of trusted virtual machine images. The best alternative is the ability to provide your own virtual machine image conforming to internal policies.

Best Practice - The best practices available to harden host systems within DMZs should be applied to virtual machines. Limiting services available to only those needed to support the application stack is appropriate.

Best Practice - Securing inter-host communications must be the rule; there can be no assumption of a secure channel between hosts, whether in a common data center or even on the same hardware device.

Best Practice - Managing and protecting application credentials and key material are critical. Extra care should be undertaken with the management of files used for application logging and debugging, as the locations of these files may be remote or unknown and the information could be sensitive.

***Best Practice* -** Account for external administration and multi-tenancy in the application's threat model.

***Best Practice* -** Applications sufficiently complex to leverage an Enterprise Service Bus (ESB) need to secure the ESB directly, leveraging a protocol such as WS-Security. The ability to segment ESBs is not available in PaaS environments.

***Best Practice* -** Metrics should be applied to assess effectiveness of application security programs. Among the direct application security-specific metrics available are vulnerability scores and patch coverage. These metrics can indicate the quality of application coding. Indirect data handling metrics, such as the percentage of data encrypted, can indicate that responsible decisions are being made from an application architecture perspective.

Best Practice - Cloud providers must support dynamic analysis web application security tools against applications hosted in their environments.

Best Practice - Attention should be paid to how malicious actors will react to new cloud application architectures that obscure application components from their scrutiny. Hackers are likely to attack visible code, including but not limited to code running in the user

Best Practice – Think:

- **Protect** - Stop bad elements from infiltrating and entering protected systems. It is critical to have defenses that block malicious software and unauthorized access. Along with baseline configuration standards established and monitored to prevent deviation and noncompliance that can create vulnerabilities in the system.

- **Detect**: To effectively detect and deter cyber threats, monitoring and analysis tools must provide an overall picture of an environment's security status. This means not only detecting attacks at the network perimeter but also identifying internal threats—whether suspicious activities or system weaknesses caused by drift away from defined security configurations.

- **Respond**: In the unfortunate event that your system may have been compromised. During this phase, you should have the tools and resources ready to go so you can quickly assess and mitigate damages. Recovery: This step is critical to getting systems back to speed and understanding how to protect and assess vulnerabilities in your system to prevent future incidents.

Best Practice - Use code analysis programs, for static and dynamic code analysis. Validate inputs and content injection and other types of attacks. When using third party testing services validate object code and test it thoroughly.
Standards - Use standards such as BSIMM2 building security in Maturity model, SAMM Software assurance Maturity Model or Systems security Engineering Capability Maturity Models.

2.2.3.4. Identity, Authentication, Authorization, etc. – all the same good stuff that applies in the enterprise applies in the cloud with the added complexity of dealing with a third party environment at any of the IaaS, PaaS, or SaaS levels of deployment.
Best Practice - Understand how cloud applications will provision accounts to users, power users and administrators - triggers for these could be links to internal enterprise systems. They should have the ability to accept claims and assertions (identifiers and attributes) from a variety of sources and entities e.g. SAML, WS-FED etc. based on standards.

Best Practice – There should be an ability to make risk based entitlement decisions about access to and within the cloud application, based on Identity and attributes of all entities (users, devices code, organization, agents) in the chain. This includes a rich risk based entitlement language leading to access management (authoring/distribution/update etc.) for protected resources.
Best Practice – there needs to be support for internal security and regulatory compliance requirements, such as claims based authentication or at the minimum role based access control.
Best Practice – Perform user activity monitoring, logging and reporting as dictated by internal policies and regulatory requirements such as SOX, PCI and HIPAA.

Best Practices – Authentication:

- Authentication for enterprises - Enterprises should consider authenticating users via their Identity Provider (IdP) and establishing trust with the SaaS vendor by federation.
- Authentication for individual users acting on their own behalf - Enterprises should consider using user-centric authentication such as Google, Yahoo, OpenID, Live ID, etc., to enable use of a single set of credentials valid at multiple sites.
- Any SaaS provider that requires proprietary methods to delegate authentication (e.g., handling trust by means of a shared encrypted cookie or other means) should be thoroughly evaluated with a proper security evaluation.
- For IaaS, authentication strategies can leverage existing enterprise capabilities.
- For IT personnel, establishing a dedicated VPN will be a better option, as they can leverage existing systems and processes. Some possible solutions include creating a dedicated VPN tunnel to the corporate network or federation. A dedicated VPN tunnel works better when the application leverages existing identity management systems (such as a SSO solution or LDAP based authentication that provides an authoritative source of identity data).
- In cases where a dedicated VPN tunnel is not feasible, applications should be designed to accept authentication assertions in various formats (SAML, WS-Federation, etc), in combination with standard network encryption such as SSL. This approach enables the organizations to deploy federated SSO not only within an enterprise, but also to cloud applications.
- OpenID is another option when the application is targeted beyond enterprise users. However, because control of OpenID credentials is outside the enterprise, the access privileges extended to such users should be limited appropriately.
- Any local authentication service implemented by the cloud provider should be OATH compliant. With an OATH-compliant solution, companies can avoid becoming locked into one vendor’s authentication credentials.
- In order to enable strong authentication (regardless of technology), cloud applications should support the capability to delegate authentication to the enterprise that is consuming the services, such as through SAML.

- Cloud providers should consider supporting various strong authentication options such as One-Time Passwords, biometrics, digital certificates, and Kerberos. This will provide another option for enterprises to use their existing infrastructure.

Best Practice - Identity as a Service should follow the same best practices that an internal IAM implementation does, along with added considerations for privacy, integrity, and auditability.

Best Practice - For internal enterprise users, custodians must review the cloud provider's options to provide secured access to the cloud, either through a direct VPN or through an industry standard such as SAML and strong authentication. The reduction of cost from using the cloud needs to be balanced against risk mitigation measures to address the privacy considerations inherent in having employee information stored externally.

Best Practice -For external users such as partners, the information owners need to incorporate interactions with IAM providers into their SDLC, as well as into their threat assessments.

2.2.3.5. Application Security – the interactions of the various components with each other, and the vulnerabilities created thereby (such as SQL Injection and Cross Site Scripting, among many others) – must also be considered and protected against.
Best Practice - PaaS customers should research the extent to which DaaS vendors support industry standards for provisioning, authentication, communication about access control policy, and audit information. Proprietary solutions present a significant risk for components of IAM environments in the cloud, because of the lack of transparency into the proprietary components. Proprietary network protocols, encryption algorithms, and data communication are often less secure, less robust, and less interoperable. It is important to use open standards for the components of IAM that you are externalizing.
Best Practice - For IaaS customers, third-party images used for launching virtual servers need to be verified for user and image authenticity. A review of the support provided for life cycle management of the image must verify the same principles as with software installed on your internal network.

2.2.3.6. Virtualization Security – Virtualization services allow multiple isolated operating systems and applications to reside on the same physical hardware

Best Practice - Identify which types of virtualization your cloud provider uses, if any. Virtualized operating systems should be augmented by third party security technology to provide layered security controls and reduce dependency on the platform provider alone.

Best Practice - Understand which security controls are in place internal to the VMs other than the built-in hypervisor isolation — such as intrusion detection, anti-virus, vulnerability scanning, etc. Secure by default configuration must be assured by following or exceeding available industry baselines.

Best Practice - Understand which security controls are in place external to the VMs to protect administrative interfaces (web-based, APIs, etc.) exposed to the customers.

Best Practice - Validate the pedigree and integrity of any VM image or template originating from the cloud provider before using.

Best Practice - VM-specific security mechanisms embedded in hypervisor APIs must be utilized to provide granular monitoring of traffic crossing VM backplanes, which will be opaque to traditional network security controls.

Best Practice - Administrative access and control of virtualized operating systems is crucial, and should include strong authentication integrated with enterprise identity management, as well as tamper-proof logging and integrity monitoring tools.

Best Practice - Explore the efficacy and feasibility of segregating VMs and creating security zones by type of usage (e.g., desktop vs. server), production stage (e.g., development, production, and testing) and sensitivity of data on separate physical hardware components such as servers, storage, etc.

Best Practice - Have a reporting mechanism in place that provides evidence of isolation and raises alerts if there is a breach of isolation.

Best Practice - Be aware of multi-tenancy situations with your VMs where regulatory concerns may warrant segregation.

2.2.3.7. Cloud Encryption and Key Management

Best Practice - Use encryption to separate data that is just being stored from data while it is used – this minimizes the attack surface.

Best Practice - Segregate the key management from the cloud provider hosting the data, creating a chain of separation. This protects both the cloud provider and customer from conflicts when compelled to provide data due to a legal mandate.

Best Practice - When stipulating encryption in contract language, assure that the encryption adheres to existing industry and government standards, as applicable.

Best Practice - Understand whether and how cloud provider facilities provide role management and separation of duties.

Best Practice - In cases where the cloud provider must perform key management, understand whether the provider has defined processes for a key management lifecycle: how keys are generated, used, stored, backed up, recovered, rotated, and deleted. Further, understand whether the same key is used for every customer or if each customer has its own key set.

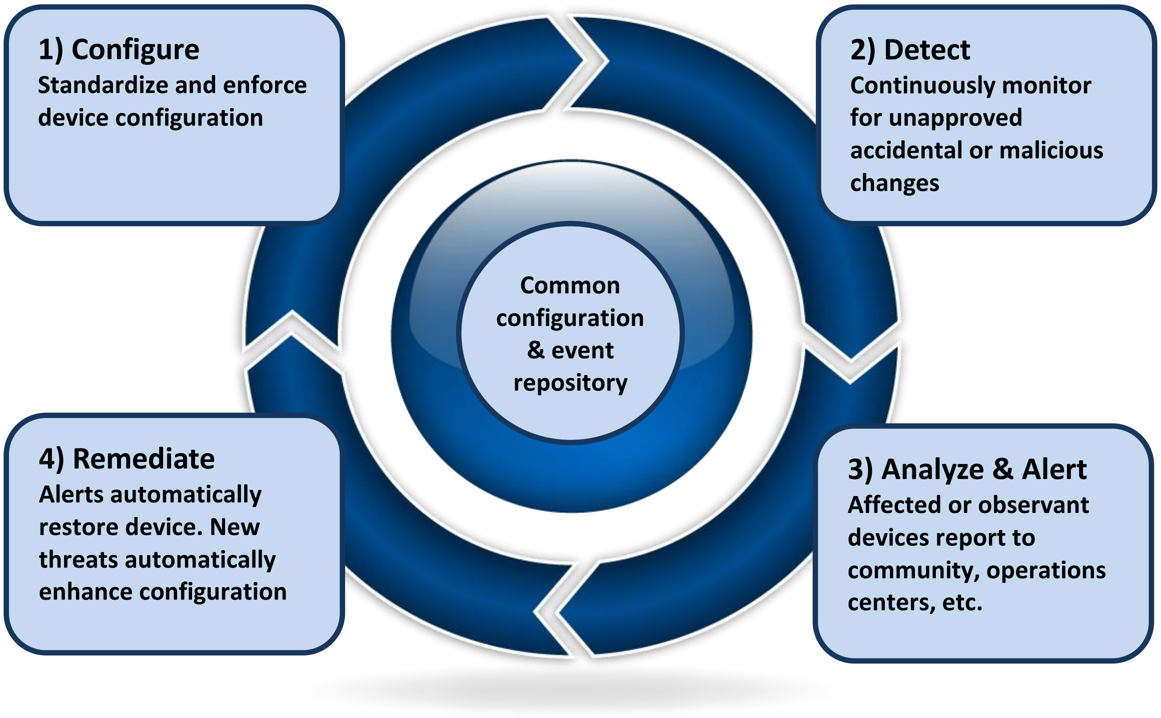
Best Practice - Assure regulated and/or sensitive customer data is encrypted in transit over the cloud provider's internal network, in addition to being encrypted at rest. This will be up to the cloud customer to implement in IaaS environments, a shared responsibility between customer and provider in PaaS environments, and the cloud provider's responsibility in SaaS environments. In IaaS environments, understand how sensitive information and key material otherwise protected by traditional encryption may be exposed during usage. For example, virtual machine swap files and other temporary data storage locations may also need to be encrypted.

2.3. Platform Protection - Secures and protects the runtime components necessary for a subject to interact with resources and/or data.

Note: There is significant overlap between client, server and storage protection requirements. At some point they are all variations on computers that have some different capabilities to match their roles. All of them need protection from malware and all of them should present as small of an attack surface as possible as well as limiting access as much as possible.

Best Practice – Management of all platforms should be automated as much as possible. This automation can be thought of as a cycle.
Stage 1 Configuration Control - First it's necessary to standardize and enforce device configurations using policy driven mechanisms. There are many standards already in place in this area and new ones being developed. These include: NIST SCAP, NIST CAESAR-FE, Open Group ACEML, and protocols from the IETF NEA, MILE and (soon to be) SACM Working Groups.
Stage 2 Detection – Any unauthorized change in a system should be detected or prevented. Relevant standards for prevention and detection include the TPM and MTM from the TCG and protocols from the IETF NEA Working Group.
Stage 3 – Analyze & Alert – When configuration deviations are detected, alerts should be sent to human operators, centralized monitoring services and other machines as necessary. The IETF INCH and MILE working groups have produced secure protocols for protecting and transmitting these messages.
Stage 4 – Remediation – Remediation is typically a manual process. However as attacks increase in speed and quantity, there is a need to fully automate this process so that the messages generated in Stage 3 can drive an automated remediation. Currently the IETF NEA protocols support several levels of response including notification, quarantine, and remediation. This step then feeds back into Stage 1 with a newer configuration that includes the fix for the attack.

Central to these four stages is an event repository that they can publish events to and subscribe to for updates. The current recommended standard is IF-MAP from the TCG. These four processes are done today, It's just that they are connected by humans and not automated. The real best practice is to connect them into an iterative cycle as shown below:


1) Configure
Standardize and enforce device configuration
2) Detect
Continuously monitor for unapproved accidental or malicious changes
Common configuration & event repository
4) Remediate
Alerts automatically restore device. New threats automatically enhance configuration
3) Analyze & Alert
Affected or observant devices report to community, operations centers, etc.

2.3.1. Client Protection - Provides the appropriate controls to ensure client devices (e.g., laptop, virtual workstation, and mobile platforms) used to access data is adequately secured and protected.

Best Practice - Secure OS by engaging self-validation at every boot-up. This assures uncorrupted code in the Boot stack.

Best Practice – Secure applications by engaging self-validation. This assures uncorrupted code is performing intended protection.

Best Practice – Launch security applications early in the boot process. This protects against malware that injects executable code prior to countermeasures (which could render them ineffective).

Best Practice - Secure firmware code and updates by requiring certified access or modification

Best Practice - Require partners and 3rd parties to use a separate workstation when connecting to the enterprise. Define and enforce a standard set of security minimums for these workstations, and engage access control lists that perform system as well as user verification to assure a safe system and a safe user.

Best Practice - Limit administrators on the local PC. (time and again, this has proven to be a weak level of protection, but it is widely popular and better than nothing).

2.3.1.1. Anti-Malware (including AV, Spam protection, etc.) - Detects, remediates, and reports any unauthorized technology (a virus, trojan, worm, exploit) embedded in or attached to operating systems, executable programs, scripts, or data files in order to compromise a system or integrity of the data used by that system

Best Practice – Secure applications by engaging self validation.
Best Practice - Use application whitelisting to identify authorized software.
Best Practice - Implement spam blockers for email.
Best Practice - Implement virus and malware scanning on each workstation
Best Practice - Launch Anti-Malware at earliest point in the boot process.

2.3.1.2. Hardening & Health Check - Ensures that all of the predefined technical components used to ensure the integrity and security of a system and its data are present, valid, and operating on the client device
Best Practice - Secure OS by engaging self validation at every boot-up.
Best Practice - Perform scheduled and on-demand executable code Health Checks to validate integrity between systems before allowing communication. Health checks can be used prior to gaining network access and also for protecting specific applications once network access is granted.
Best Practice - Develop and enforce a set of endpoint security software applications (e.g., OS, Desktop) and workstation configuration that has been pre-approved.
Best Practice - Automatically correct corrupted components
Best Practice - Validate encrypted OS file hash with known hash and store validation hash in secure location (i.e. TPM).

2.3.1.3. Port & Device Control - Restricts or enables the use of certain ports, protocols, or devices (logical or physical) available on a client device
Best Practice – Use traffic monitoring software that tracks application and port/device traffic, looking for anomalies.
Best Practice – Develop high security systems that are appropriate for sensitive usage. Engage port and device control measures beyond the standard workstations, to strengthen system protection. When necessary, use whitelisting to lock down permitted executables.
Best Practice – Turning off all risky or unnecessary ports and monitoring all necessary ports can prevent or detect malware from exfiltration data. While this is a popular system hardening technique, we're not sure how effective it is.

2.3.1.4. Data Protection – Client support for data protection
Best Practice - Require two-factor authentication for local PC access.
Best Practice - Use CITRIX/VDI to prevent transferring data out of the enterprise.
Best Practice - Implement whole disk encryption to protect data if the workstation is stolen. Refresh next generation of PCs with self-encrypting drives conforming to the TCG standard. Until then deploy software based drive encryption.
Best Practice -Implement Disk Wipe as part of the process when machines are decommissioned. Machines with more sensitive data should have their disks physically destroyed.
Best Practice - Utilize Software based encryption until Hardware systems have mature management tools.

2.3.1.5. Virtualization - Provides a logical separation of data, programs, or processes from the physical hardware

Best Practice – Consider new technology that creates a virtual “sandbox” for each application that is aware of the application standard operations and prevents non-standard or risky actions.
Best Practice - Create USB based self-contained bootable devices to generate virtual systems. These systems are short lived targets, with self-validation and isolation from the host system.
Best Practice - Perform self-validation of virtual systems.
Best Practice - Assure complete isolation from host hardware.
Best Practice -Utilize systems as required and shut them down when not in use.

2.3.2. Host Protection - Provides the appropriate controls to ensure hosts (e.g., servers, mainframes) and storage devices (e.g., disk arrays, SAN, NAS) used to access data is adequately secured and protected.

2.3.2.1. Anti-Malware - Detects, remediates, and reports any unauthorized technology (a virus, trojan, worm, exploit) embedded in or attached to operating systems, executable programs, scripts, or data files in order to compromise a system or integrity of the data used by that system
Best Practice – Very similar considerations that apply to client devices apply here. Do not neglect servers when deploying enterprise anti malware suites. Additional traffic monitoring software should be engaged as well.

2.3.2.2. Hardening - Locks down a host (e.g., server, disk array, network storage) in order to minimize the attack surface by disabling or removing unused, unnecessary, or risky components
Best Practice- Tag sensitive data and engage appropriate increased protection levels where necessary*. Use specifically enhanced security hosts for sensitive data.*
Best Practice- Lock down file shares to prevent guest or anonymous access.
Best Practice - Require two-factor authentication where available; complex passwords otherwise.
Best Practice - Restrict privileges to only those that are essential to complete the assigned Statement of Work.
Best Practice - Use jump servers to manage rather than allowing any client to connect directly to a host.
Best Practice - Lock down DBLinks, etc to ensure database level exploit paths do not exist.
Best Practice -Provide each administrator his/her own privileged account.
Best Practice - Log sufficient detail to track user actions and alert on error conditions.

2.3.2.3. Health State - Ensures that all of the predefined technical components used to ensure the integrity and security of a system and its data are present, valid, and operating on the client device
Best Practice – Run complete host scans and mitigate any findings.
Best Practice – Lock down configurations using policy based tools to control configuration state and alert when changed.

2.3.2.4. Virtualization - Provides a logical separation of data, programs, or processes from the physical hardware

Best Practice - Perform self-validation of virtual systems.
Best Practice - Assure complete isolation from host hardware.

2.3.3. Storage Protection - Provides the appropriate controls to ensure hosts (e.g., servers, mainframes) and storage devices (e.g., disk arrays, SAN, NAS) used to access data is adequately secured and protected.

2.3.3.1. Archive - Ensures that data archive systems are configured provide appropriate access control from authorized

Best Practice – Encrypt data prior to archiving. Ensure that keys will be available when recovery is needed. For long term storage, use cryptographic algorithms that will retain their strength as long as protection is required.
Best Practice – Prepare for migration. Data stored for a long time will have to be periodically migrated to newer systems to ensure future availability. Migration needs to be capable of happening at the physical media layer, at the operating system layer, at the application later and at the cryptographic protection layer.

2.3.3.2. Backup & Recovery - Ensures that Backup systems are configured provide appropriate access control from authorized hosts, and that data restoration is only permitted to authorized systems

Best Practice – Test! Periodically test the ability to recover information.

2.3.3.3. Network Attached Storage (NAS)

Best Practice - Ensure that Network Attached Storage systems are hardened to minimize network attack surface, and provide appropriate access control to stored data files.

2.3.3.4. Storage Area Network (SAN)

Best Practice - Ensure that Storage Area Networks are configured provide appropriate access control from authorized hosts, and their storage management systems are configured to resist attack.

2.3.4. Mobile Device Security – Provide data protection and other security devices for smart phones, tablet computers and other emerging non-tradition platforms.

Best Practice – Use device encryption. All devices that contain company data should be managed under a Mobile Device Management system that enforces appropriate policies.
Best Practice – use a strong password to unlock the device.
Best Practice – Limit access to sensitive data.
Best Practice – Use device aware connections that will enforce access control rules.
Best Practice - Uninstall any unnecessary installed by the handset maker or the carrier.
Best Practice – Limit the use of preinstalled applications that expose data to the device API.

2.3.4.1. Secure Data Container – When these devices are used for both personal and business functions there needs to be an internal container to separate the data and applications

Best Practice – ensure secure container is encrypted. Minimize (or eliminate) business applications that contain data that is outside of the secure container.
Best Practice - Leverage a “secure container” application that is not decrypted with the device unlock credential.
Best Practice - Once data from a “secure container” app data has been decrypted, additional measures should be taken to limit the exposure of the decrypted data.
Best Practice - User education: Users should understand that any data they input into the pre-installed apps may be shared with other apps with access to the Application programming interface.

2.3.4.2. Secure Authentication - authenticating both the device and user.

Best Practice - Ensure that the device that is connecting to your network is authorized. Ensure that user authentication meets enterprise requirements. We prefer to factor authentication where the private key is protected by a smart card or a TPM chip. If this is not available, hardware based one-time password tokens can be used. Passwords, soft certificates, or software based one-time password tokens should not be used.
Best Practice – Access credentials should not be exportable.

2.3.4.3. Dynamic Device Management

***Best Practice* –** use some form of dynamic device management service to ensure that all devices are compliant with security policies

2.3.5. Industrial Control Systems (ICS) Protection – ensure that factory automation systems, machine tools, SCADA devices, and other industrial control systems are protected from cyber attacks

Best Practice - Ensure that factory automation systems, machine tools, SCADA devices, and other industrial control systems are protected from cyber-attacks. Industrial Control Systems often utilize components and protocols that lack even the most basic security functionality such as encrypted passwords, host intrusion detection functionality and anti-spoofing protection for communications. To the degree it is possible, modern control systems components should be selected for new systems; however, even the latest products from some vendors in this space may still lack basic security functionality. Industrial control systems typically have multi-decade lifecycles; replacing these systems to improve security is often cost prohibitive. Instead, the available built-in security controls for a given system is combined with external controls which provide layers of network isolation, protocol filters, and end-user authentication and authorization.

Standards - The industry best practices for the security architecture is were developed within the International Society for Automation (ISA) Standards Development Committee 99, "Industrial Automation and Control Systems Security." A set of Technical Standards from this ISA 99 committee are available as the IEC 62443 series of Technical Standards.

Additional security architecture and standards for protecting ICS devices is in development being developed by both the ISA100 committee ("Wireless Systems for Automation") and by the Trusted Computing Group. ISA100 recently published a technical architecture document which defines a framework which can be used to describe the components, connectivity, threats and risks associated with ICS components communicating over untrusted or unreliable communications media. The Trusted Computing Group (TCG) is actively developing a protocol standard for managing and protecting ICS devices from these untrusted transport networks.

2.3.5.1. Malware Protection – Ensures that malware, and other attacks via the network do not impact ICS devices

Best Practice – ICS systems have a very long lifespan. They form a significant part of the critical infrastructure. They typically use weak, proprietary network protocols and the devices themselves have weak operating systems. These systems are being rapidly connected to the Internet for convenience without regard to their security vulnerabilities. Since the proprietary protocols and operating systems can't easily be changed, the only real solution is to connect them via another box that does have protection. These boxes (sometimes called "middle boxes") talk to the ICS on one side and to conventional networks on the other. The Trusted Computing Group (TCG) sub group – Trusted Network Connect (TNC) has created a set of standards and an architecture for these middle boxes. Deployment of these middle boxes as an isolation barrier can protect many ICS and SCADA systems form malware, probing and attacks coming from the Internet.

Best Practice - Ensure that malware, and other attacks via the network do not impact ICS devices Since ICS devices are often many years old, their designs may often build upon systems and platforms which are both out of date and insecure. For example, if a 10 year old ICS human-machine interface HMI) device was implemented on a Windows2000 platform, there are known security vulnerabilities which cannot be fixed because Windows2000 is an end-of-life product. Even if new fixes were to become available, many systems must be recertified before such fixes can be installed into the production operations environment. In situations such as that described above, the industry best practices rely on installing as many patches as possible (outages, for example, at an oil refinery may be rare and expensive) and providing as much isolation between these systems and other (IT) systems as possible.

2.3.5.2. Denial of Service Protection – Ensures that ICS systems continue to function when under attack

Best Practice – Use of the middle boxes mentioned above can block some denial of service attacks. An even better approach is to disconnect these devices from the Internet completely – including extensions of the internet into corporate networks. A set of ICS systems could still be connected by a local network, but all usage and administration would need to be done directly on that network. While this is counter to the current trend there are several nations and enterprises that are moving this direction as part of their defense. And while a disconnected network is pretty secure, it can still fall victim to attacks done via manual connections – typically plugging the same laptops or USB drives into an Internet connected network and then into the isolated network.

Best Practice - ICS systems often have very high availability requirements: non-stop operation for multiple years is not uncommon. Denial of Service can disrupt these operations, causing loss of productivity and potentially causing physical systems damage (e.g., an explosion at a refinery or along an underground fuel pipeline). The industry best practices around ICS DoS protection center upon the creation of communications paths for inter-connected ICS components that are isolated from the wider Internet community. The architecture for these paths is described in the ISA99 documents discussed above. Redundant communications paths (for example, making available both WiFi and Cellular communications capabilities) help protect against non-common-mode failures. Additionally, well-tested and documented backup and restore capability is also critical to getting the system back to a known-good state should an attack (DoS or otherwise) occur that removes or corrupts the operating code in the ICS devices.

2.3.6. Network Protection - Provides the appropriate controls to ensure network devices (e.g., switches, routers, gateways, network cables) used to access data is adequately secured and protected. Network controls also ensure that authenticated users are only able to access networked resources for which they are authorized.
Best Practice - Segment the network; don't create a flat network. Separate entities of differing trust levels; don't put suppliers, customers, employees, and beneficiaries together.
Best Practice - Log sufficient detail to track user actions and alert on error conditions.
Best Practice - Filter network access wherever possible; base network reachability on data/application access needs.

Evolving Best Practice*:* Historically network protection has been accomplished by deploying multiple session-based security control systems in a defense in depth manner, including packet filters and proxies, which still remains true today. However, over a decade ago the Jericho Forum observed that historic enterprise perimeter defense was being challenged by business requirements that non-employees access corporate network resources. The more porous the perimeter becomes from those uses the more challenged session-based control systems become to provide effective network protection. Session-based controls have become even more challenged recently due to the emergence of the "cloud" and "device commoditization" (e.g., mobile computing devices possibly including the concept of Bring Your Own Device) technologies coupled with the increasing realization regarding the security dangers associated with "flat networks" (i.e., the need to evolve the corporate network into sets of secured enclaves). Because of these vectors, industry is gradually realizing that identity is the new perimeter. Therefore, rather than network controls being based upon sessions, they instead need to become based upon Identity and Access Management (IAM) techniques. IAM needs to be enforced both at the perimeter but, more importantly, at numerous points within the corporate network itself.

Even though this algorithmic sea change has been slowly emerging, it is currently unclear what the specific final target goal of IAM should be. It is well recognized that "Identity" in this new algorithm includes human identity, preferably human identities established by two (or more) factor authentication (because the old account-password approach is far too easily subverted). (Human identities should be authenticated with PKI within smart cards.) However, "identity" must also include device identity: one needs to know who owns that computing device (e.g., our company or someone else). Because of the prevalence of *pwned* devices, identity should also include device health (e.g., remote attestation). Lastly, it is increasingly recognized that identity should also include other identity spaces such as application identities. Because authentication, authorization, and network access control increasingly involves multiple identity spaces, IAM enforcements therefore are becoming based upon a combination of identity spaces as determined by local policies. Because the same business requirements that created de-perimeterization involve associations outside of the historic corporate perimeter (e.g., "cloud" as well as cooperating peers, customers, and suppliers), Federated Identity Management (e.g., OMB M-04-04 and NIST SP 800-63-1) also is an integral part of the new "Identity is the Perimeter" algorithm.

A possible technology target for that latter approach is the Trusted Computing Group's (TCG) Trusted Network Connect (TNC) Architecture, protocols, and conforming products – and equivalent IETF standards (e.g., Network Endpoint Assessment (NEA)).

Basic principles around de-perimeterization are described in the Open Group Jericho Forum's Commandments - https://www2.opengroup.org/ogsys/catalog/W124 and self-assessment guide - https://www2.opengroup.org/ogsys/catalog/G124 .

2.3.6.1. **Enclaves** - Controls network access to/from a collection of resources (hardware, software, applications, and data) operating under the control of a single authority which are logically isolated from the intranet by a Policy Enforcement Point (PEP) through which all traffic into and out of the access zone or enclave must pass.

Standards - Standardize on OASIS' XACML to convey policy decision point (PDP) information to PEPs. Standardize on OASIS' SAML to convey authentication results to support single sign on (SSO) and Federated identity management capabilities.

Best Practice - Replace flat network infrastructure with a segmented networks in which the corporate networks are changed into sets of secured enclaves. Restrict network communications to authorized accesses determined by authentications using the combination of human identity plus device identity, the results of machine health checks and also the results of policy based authorization decisions.

2.3.6.2. **Encryption** - Transforms data in motion using cryptography to produce ciphertext which is not human readable and which may not (for appropriate reasons) be decipherable
Best Practice – encrypting networks at the lower layers provides some degree of isolation and security from unwanted guests.

2.3.6.3. **Firewall** - Enforces a boundary between two or more network segments to prevent tampering, unauthorized access, and data leakage

Best Practice – Firewalls are best for protecting the enterprise from unwanted traffic – basically making sure that network based resources are available. Attempts to do fine grained access control at firewalls do not scale, nor do they protect the data once it has left.

2.3.6.4. Filtering - Limits access to network segments through the use of policy decision points, policy enforcement points, and any required data (e.g., user, network segment, policy) which may be integrated directly into the network appliances
Best Practice – Filtering access at the network layer is an economical way to create enclaves and provide some isolation between different user populations. Filtering should not substitute for data protection.

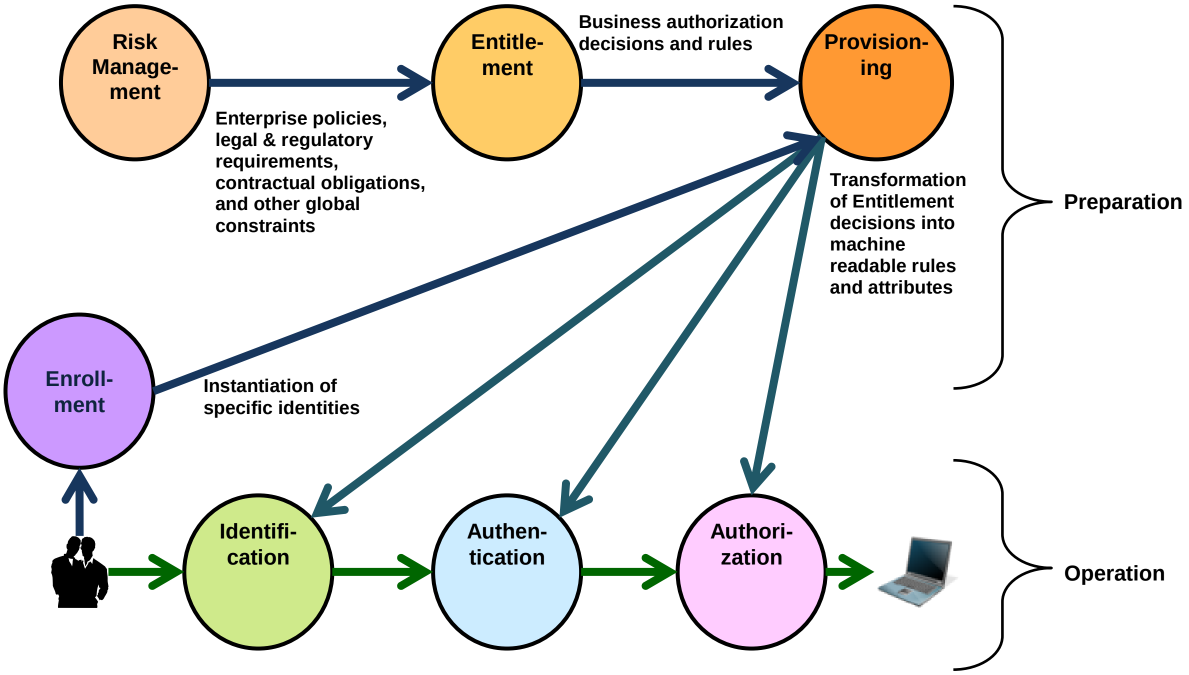
2.3.6.5. VPN, Gateway & Proxy - Components that serve as a means to securely cross network boundaries by accepting connections from a client device, ensure that authentication and authorization requirements are satisfied before permitting the client into the targeted security domain, and complete a connection on behalf of the user to a remote destination. Includes client-oriented VPN sessions/terminations from remote less trusted networks
Best Practice - Use VPNs in tunnel-all mode. Do not use split tunnels – migration form split tunnel implementations is very difficult.
Best Practice - Require the use of secure protocols from the VPN to hosts, databases, etc.
Best Practice - Require two-factor authentication for VPN access.

2.3.6.6. Hardening - Locks down a network device or appliance (e.g., router, switch, gateway, proxy) in order to minimize the attack surface by disabling or removing unused, unnecessary, or risky components
Best practice – Network components have complex operating systems and should be protected from malware and overt attacks just like any other computer. In particular, their authentication systems are often weak and additional protection needs to be applied. One way this can be done is by placing administration interfaces on non-routable subnets.

2.4. Access Control Services – (sometimes referred to as IAM –Identity and access Management)

Manages the data required to track, authenticate, and authorize a subject's (e.g., person, application, device) access to one or more resources (e.g., client, host, network, application).

Before describing Access control services, it’s important to set them fully in context. Most security controls are designed to either detect intruders or prevent access to data and other resources. The systems that make up access control services are specifically designed to allow access for legitimate users. As such they are constructed of a number of gates or filters – whose goal is to allow those users in while rejecting unauthorized attempts. An enterprise access control system requires a number of services to be in place prior to use. They also require an enrollment service to register new users. And finally there are a set of operational services that an enrolled user interacts with. These are shown below and will be described after the illustration.


Risk Manage-ment
Entitle-ment
Business authorization decisions and rules
Provision-ing
Enterprise policies, legal & regulatory requirements, contractual obligations, and other global constraints
Transformation of Entitlement decisions into machine readable rules and attributes
Preparation
Enroll-ment
Instantiation of specific identities
Identifi-cation
Authen-tication
Authori-zation
Operation

Risk Management – While there are many risk management processes running at different levels in a typical large enterprise, in this context, risk management refers to enterprise wide corporate decisions that result in constraints to an access control system. Examples include a decision to be compliant to export control laws, privacy regulations, corporate decisions on outsourcing locations and other decisions that directly affect access control. These decisions are made at the corporate executive level.

Entitlement – This is a local process of deciding which entities (people, devices, applications, etc.) get access to which data and resources. These are also business decisions. They are constrained by the Risk Management decisions and impose further constraints or refinements on access. These decisions are typically made at a program, project or work unit level. Note that the term *Entitlement* is also used to apply to technical access control decisions. In this case the term is referring to business decisions and business policies, not technology.

Provisioning – Once the business decisions are made the Enrollment process translates them into machine readable rules. These rules are then applied to the various components of an access control system via Policy Administration Points (PAP) – which are described below. Currently translation is specific to products.

> ***Needed Standard*** – A general purpose mechanism for translating business rule into machine readable policies that interoperates across vendors, allowing an enterprise to centrally manage the creation of authorization rules. The OASIS XACML standard

describes the output, what's lacking is a human readable language and tool set for business people to create the input.

Enrollment – This describes the process of adding users, devices, applications, and any other entity that requires access, to the access control system. This is where accounts are created, certificates generate, passwords initialized, etc. This is where attributes are verified and levels of assurance for credentials are applied based on the integrity of those attributes. Enrollment processes tend to also be specific to products, although there are some general purpose enrollment tools available from vendors. There are also tools that combine the functions of Provisioning and Enrollment.

Identification – The first stage in the operational services, Identification is the process an entity goes through when desiring access to a resource. The person, machine, application, etc. presents a token containing an *Identifier* and the system checks to see if that identifier is registered.

Authentication – This is the process of verifying that the identifier presented correctly identifies the person (or machine or application) that is requesting access. The strength of this authentication is often used when deciding how much access the person will be granted. Successful authentication, by itself, should not grant access to resources.

Authorization – Once the user has been authenticated, a final process takes place that decide what resources to grant access to. This authorization decision is based on properties of the resource, properties of the requestor, the type of access requested, and other factors such time of day or location.

Since the first two processes (Risk Management & Entitlement) are very business specific and the next two (Provisioning & Enrollment) are – until we have better standards – very application specific they are not developed further. The last three (Identity Management – including Identification – and parts of Enrollment, Authentication, and Authorization) have more detailed sections below. Directory services – critical for authentication and authorization decisions, has been broken out as a separate section. While the main treatment of Audit services is under authorization, logging and keeping audit records are important for all of these steps.

Best Practice – Ensure that architects, developers and others who build or buy systems understand the differences between Identity Management, Authentication, and Authorization. Identity Management includes the creation and use of Identities in an Identification process.

Identification answers the question “Who are you?” while ***Authentication*** addresses the statement “Now that I know who you are, prove it.” And ***Authorization*** addresses the statement “Now that I know who you, this is the access you will get to the requested resource.” At a logical level this is a sequential process and these three concepts will be dealt with in this order. However there are valid cases where no identification or authentication is necessary. And there are use cases for anonymity and pseudonimity.

***Best Practice* -** Use a self-service request model for managing access. This includes the establishment of identities as well as requesting access to specific resources. The advantage of doing this is that it typically shortens the time required to gain acceptable access credentials.

***Best Practice* –** These systems need to be carefully protected. They are the gateways to enterprise data and resources.

Over the years we’ve spent lots of time worrying about the security characteristics of various types of authentication tokens, with broad consensus that static passwords reek. And we’ve put lots of thought into the processes we use to vet users’ identity and to bind tokens to users. And of course we’ve put lots of effort into lifecycle management and processes to disable authenticators when they are no longer needed. NIST Special Publication 800-63-1 is a pretty good exploration of topics like those mentioned above, and describes how they contribute to an authentication event’s level of assurance. However, it’s time to also focus on the back end systems that support these authenticators.

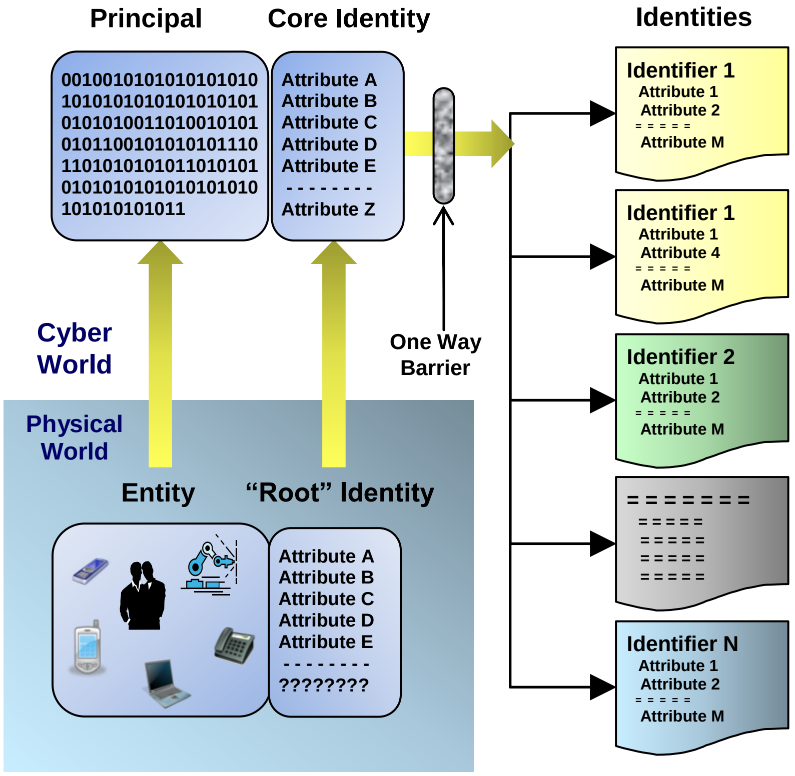
We’ve progressed far enough that the authentication back-end systems have now become attractive attack points. Why should attackers try to steal someone’s smart card if they can steal the certificate authority’s certificate signing key? Why should attackers try to replay a SAML assertion if they can steal the IdP’s assertion signing key? Why should attackers try to steal someone’s OTP token if they can steal all the tokens’ shared secrets from the back-end OTP verification system?

Even if attackers are unable to steal OTP tokens’ secrets from a company’s back-end OTP verification system, they may be able to steal the token secrets from the token supplier, or some third party contracted to inexpensively program OTP tokens. Even if attackers are unable to actually steal secrets and/or keys (thank heavens for hardware security modules), they may be able to compromise the back-end servers to maliciously exercise the secrets and/or keys, thereby generating what appear to be valid certificates, assertions, or OTP values. Even if attackers are unable to maliciously exercise a back-end server’s secrets and/or keys, they may be able to inject malware onto a RADIUS, LDAP, or OTP server that returns a success status for every authentication, bind, or verification request.

Don't forget the back-end! Are your back-end authentication servers sufficiently hardened? Are they in secure network enclaves? Are your secrets and keys protected by HSMs? Are single-factor admin passwords used to control access to your multi-factor authentication systems? Are you confident that your virtual machine hypervisor doesn't open attack channels to your hosted authentication servers? Could compromised workstations used for remote administration introduce malware to your authentication servers?

2.4.1. Identity Management - Manages the creation and management of a subject's attributes that can identify them uniquely (e.g., name, group, employment status, nationality, etc.)

See below for an illustration of the definitions and component structure that make up Identities.



Terms & Definitions

Entity – A human, device, or other object that has both a separate existence and the capacity to act

Principal – An Entity capable of participating in the cyber world; for a non-human Principal often equals Entity

Attribute – A Name-Value Pair bound to a Principal. A ***Claim*** is a specific attribute use case.

Identifier – An Attribute bound to a Principal that is unique within a domain

Identity – An Identifier and zero or more Attributes bound to a Principal; a ***Persona*** is a synonym for Identity

Root Identity – All Attributes, known or unknown, of an Entity

Core Identity – All Attributes of a Principal or Cyber capable subset of Root Identity

2.4.1.1. Identifiers – provides the name that attributes can be attached to when creating an identity.

Best Practice – An identifier MUST be unique within the domain where it is used and SHOULD be globally unique and fully qualified. Standards based examples of these include the OASIS XRI format, IETF DNS naming system, and IETF E-Mail names. When an identifier's domain of use is not intuitively obvious, the identifier should be able to be more fully qualified to avoid ambiguity.

Best Practice - Even when more fully-qualified, identifiers should still be easily verbally conveyed. E.g., when calling a help center, user IDs, device IDs, and software product identifiers are commonly communicated over the telephone call.

Best Practice - Identifiers to which role/privilege data are associated should be non-re-assignable. Otherwise it's likely the roles/privileges intended for the previously represented entity will wrongly be inherited by the newly represented entity. When identifier reassignment must be supported, or when identifiers change (e.g., name-based identifiers after marriage or divorce), it's helpful to have some means of notification to alert interested parties that roles/privileges need to be corrected.

Best Practice – Identifiers should not have any meaning; they are just a locator to a record… nothing more. Identifiers should not include imbedded meaning, and superlatives should be avoided. "New" won't always be new, "nextGen" will someday be legacy, and "best" won't always be best. As meanings change, the identifiers become incorrect or misleading.

Best Practice - Use something other than the identifier as a key to a database record. This could be another attribute tied to the same Identity.

2.4.1.2. Identity Creation & Distribution - Provides access to identity data used for access decisions or personalization through a defined set of interfaces able to control access to data

Best Practice - Use a scalable architecture (naming authority, publishing authority) for managing identities.

Best Practices – Identities are composed of an Identifier and a set of attributes. Trust comes from the validation of the data in the attributes, not the identifier. Identity strength relies on the attribute verification processes used when the identity is created, the attribute to identifier binding, and the strength of the method for encapsulating the Identity.

A relying party's trust in an Identity comes from:

- The quantity and quality of the Attributes associated with the Identity
- The ability to verify Attributes when the Identity is used for access
- Documentation of the rigor of attribute validation during the creation of the Identity
- The strength of the binding between the Attributes and the Identifier
- Trust in the encapsulation, credentialing or delivery mechanisms for the proffered identity

The following Identity Principles from the Open Group Jericho Forum are relevant to creating good Identities:

1. All core identities must be protected to ensure their secrecy and integrity

Entities control disclosure of their attributes. Identities are created with a needed subset of the Entities attributes and a local, domain specific identifier. Aggregation of attributes for an entity is prevented. IdM systems should only consume attributes necessary for access decisions. Voluntary attribute disclosure must be supported. Note: an entity that limits attribute disclosure during identity creation risks access constraints from a relying party.

2. Identifiers must be able to be trusted.

Identifiers are unique within their domain of use. Identifiers are created by an authority trusted in their domain of use. This requires care in the creation of or selection of attributes that are used as identifiers.

3. The authoritative source of identity will be the unique identifier or credentials offered by the persona representing that entity.

The Entity has control over the creation of Identities or Persona. Note: A relying party may still issue constraints for acceptable attributes and corresponding Identity construction.

4. An Entity can have multiple, separate Persona (Identities) and related unique identifiers.

User must be able to select the desired Identity for specific domain. Resource owners must have the capability to require a specific Identity. Controls need to prevent Identity reuse across different domains that have different trust levels. Notes: Many current IDM systems are not flexible enough to support this. Policies are often more restrictive than technology – sometimes more for historical rather than risk based reasons. Identity reuse is a widespread practice

5. Identities or Persona must, in specific use cases, be able to be seen as the same.

This is to prevent fraud when a principal has multiple identities. And prevent a principal from substituting a weaker identity where a domain requires a stronger one. And to prevent replay attacks. Note: this requires mechanisms to aggregate specified identities without aggregating all of a principal's identities.

6. The attribute owner is responsible for the protection and appropriate disclosure of the attribute.

Limit exposure to a principal's attributes. Ensure the integrity of attributes. Ensure that attributes are accurate, complete and necessary. Note: As the level of authentication trust relies mostly on the integrity and verification of an identity's attributes, great care must be taken to establish them correctly and prevent them from corruption or unwarranted disclosure

7. Connecting attributes to persona must be simple and verifiable.

A relying party needs to be able to easily verify both content and binding of an attribute. An entity needs to be able to connect desired attributes when creating an identity. Entities need to be able to challenge incorrect attribute data. Mechanisms need to be in place to allow an entity to manage their associated attributes

8. The source of the attribute should be as close to the authoritative source as possible

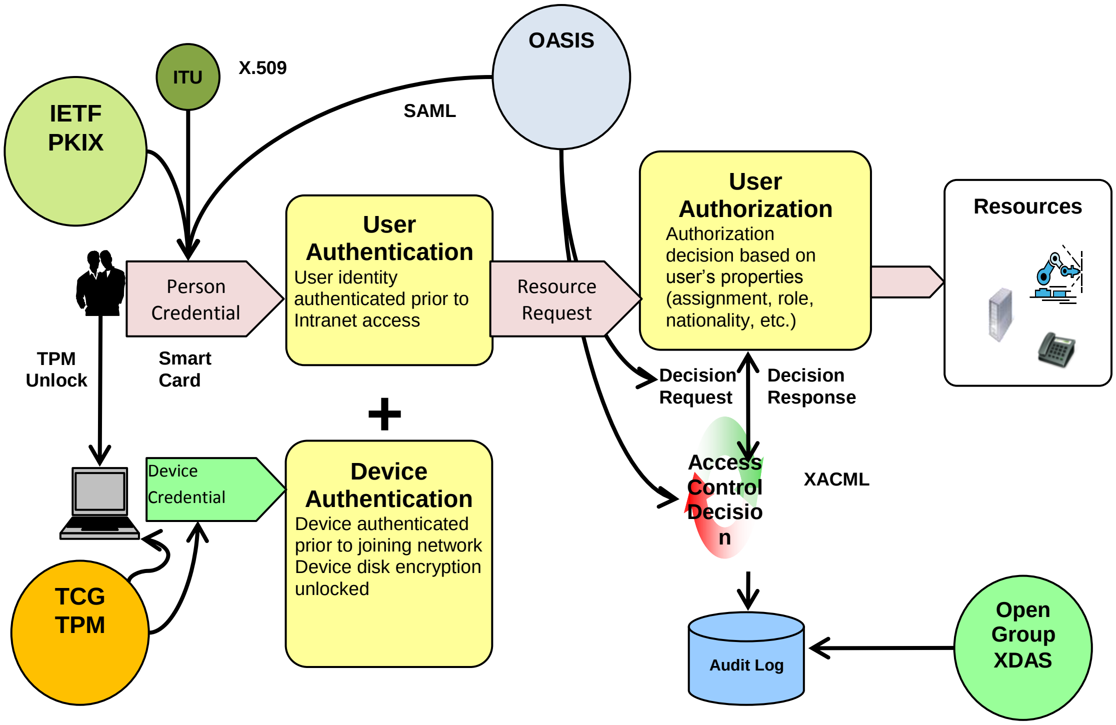
The accuracy and validity of attributes must be demonstrable and provable. Secondary attribute sources should be avoided. Both the identity creator and relying party need access to attribute sources.

2.4.1.3. Identity Registration & Naming - Creates and manages the identifier (e.g., BEMSID, XRI) and all related attributes of a subject (e.g., name, address, etc.) used for tracking a subject's actions or authorize the subject's access to a resource.
Best Practice - Use federated identities over local identities where possible.

2.4.1.4. Resource Registration & Naming - Creates and manages the identifier (e.g., App ID) and all related attributes of a subject (e.g., name, address, etc.) used for tracking resources (e.g., applications, hosts)
Best Practice - Leverage the system used to track resources (e.g., applications, servers, services) as the source for mastering resource identities rather than creating something separate for resource identities.

2.4.2. Authentication - Manages and enables the exchange of security information (e.g., passwords, certificates) in order to verify the claimed identity of the user
Best Practice – Passwords should be phased out where possible. Where devices are capable, we are replacing password use with smart cards. Where smart cards can’t be used (either because the device doesn’t support them, or in some cases they are prohibited by governments) we are using One Time Password (OTP) tokens. Between these two we are eliminating most passwords. Our OTP system uses the OAUTH standard. Smart cards use X.509 certificates. In addition to the X.509 standard, we also use the related IETF PKIX protocols, NIST 800-63 (for levels of assurance) Special Publication.
Best Practice – Use independent authentication systems for people and devices to authenticate both users and systems. This discrete dual authentication enables an authorized user to access sensitive data only from and authorized system. It also blocks access when either the user’s credentials are compromised or the system is stolen or compromised. Authentication for devices and applications are still likely to be PKI based.

Components and relevant standards are shown below.



Best Practices

- Require administrators to use separate accounts and credentials to access administrator functions.
- Externalize authentication from targets.
- Implement authentication as a dialog… not a onetime event; think risk based authentication.
- Ensure authentication events result in standard tokens that support single sign-on
- Support single sign-on (federation) across security domains.
- Prefer non-biometric factors (e.g., OTP, knowledge based credentials) in authentication as biometric credentials (e.g., DNA, fingerprints) are not revocable.

2.4.2.1. **Adaptive (Risk Based) Authentication** - Manages the assignment of credentials to users and enables non-static authentication which may include prompts to increase the level of assurance takes into account the risk associated with the requested operation and prompts (if appropriate) the user for additional authentication information to increase the level of assurance (e.g., the user is really who they claim they are)
Best Practice – Adaptive authentication results may be used as an additional factor when making an authorization decision.

2.4.2.2. **Application Integration** - Specifies the means by which resources (e.g., applications, hosts) integrate and utilize authentication services
Best Practice – Authentication externalization is preferred for applications. That way the application can leverage an enterprise authentication service. This allows for the enterprise to change authentication methods and strengths without affecting applications. It also reduces the amount of security code in the enterprise which

shrinks attack surface and reduces the possibility of coding or implementation errors and vulnerabilities.

Best Practice - You can externalize the authentication service, but you must then authenticate the service itself, and/or the signed assertions or data that is returned. You need to be constantly aware of that weakest link in your authentication and access control chain.

2.4.2.3. Assertions & Federation - Manages the assignment of credentials to users and enables inbound and outbound authentication across security domains without requiring the user to re-authenticate

Standard – OASIS SAML – Security Assertions Markup Language is our corporate standard for assertions.

Practice Gap – For consistent use of federation among organizations supporting a critical infrastructure, and their extended sets of partners and suppliers, common criteria are needed to establish the trust relationship among federates, including level of assurance of both identity and authentication. There is synergy here with item above on Adaptive Authentication. To relying parties, the authentication strength of assertions is no stronger than the weakest authentication mechanism employed at their starting points.

Practice Gap – When multiple organizations are involved in collaborative support of a critical infrastructure, the use of chained assertions across multiple organizations must be based on a common interpretation of the resulting trust complexities, and a common approach to the use and interpretation of chained assertions must be adopted by all parties. Standards or best practices should be established as guidance.

Best Practice - Prefer the assertion of a user from a trusted source rather than managing credentials in the local security domain.

2.4.2.4. Biometrics - Manages the assignment of credentials (e.g., fingerprints, DNA, retina map, voiceprint)to users and enables authentication using biometric information

Best Practice Comments – While biometrics are appealing on the surface, they have a number of limitations:

- Biometric data are not revocable
- Biometric systems are non-deterministic – that is they allow a certain amount of false positive in order to lower the amount of false negatives
- Biometric systems often require specialized and expensive hardware,
- For most biometrics, there exists population segments that cannot use that biometric,
- The entropy in biometrics is significantly less than even passwords.
- Consider the use of biometrics for platforms that do not easily support other multi-factor authentication mechanisms (e.g., mobile).

Nevertheless, a biometric may be usable when combined with other credentials. The entropy is generally equivalent to a PIN and very specialized biometric uses (such as floor based weight sensors to eliminate tailgating) do have value.

2.4.2.5. Certificate & PKI - Manages the assignment of credentials (e.g., smart cards , personal browser certificates) to users and enables authentication using public key infrastructure

Best Practice – Certificate servers need to be strongly protected. Root certificate authorities should be kept off line. All certificate authorities should have locked down administration procedures and accounts.

Best Practice – End users should not have to manage certificate stores in browsers. Organizations should configure web browsers with a trusted subset of those available.

Best Practice - For IAL4 identity assurance we have Medium Assurance Hardware based proofing and credentialing, mapped to the CertiPath aerospace trust bridge, and the U.S. Government Federal Trust Bridge. This federation requires strict governance controls, policy definition mapping, annual formal third party audits, PKI based cross-certification with explicit namespace and policy constraints and mappings. It also requires strict operational roles and trusted personnel with background checks or clearances, strict identity proofing, logging, monitoring, and monthly auditing.

2.4.2.6. Forgotten/Lost/Broken - Supports users who should be but are no longer able to authenticate using an existing credential

Best Practice – Organizations need an out of band process for restoring access credentials in these cases. The process needs to be trusted, verifiable, and flexible. Help desks area common attack vector.

Best Practice - Prevent the ability to sync passwords on all accounts; this helps to minimize the impact of an account compromise.

Best Practice - Force the user to reset a password or PIN following a help desk assisted password reset; this ensures the help desk analysts do not know the user's password or PIN.

Best Practice - Require users to complete a profile to assist with vetting the user if he/she forgets/loses all means of authenticating to the environment; this reduces costs during user-assisted password/PIN resets.

2.4.2.7. One Time Passwords (OTP) - Manages the assignment of credentials (e.g., hardware based OTP, scratch list) to users and enables authentication using one time passwords

Best Practice – OTP systems need as much scrutiny as PKI or certificate based systems. Typically, as they rely on secret key cryptography, they cannot be made as strong as PKI based authentication systems. They therefore, should not allow the same level of access. Use Certificates if possible and use OTP only where Certificates don't work.

2.4.2.8. Passwords - Manages the assignment of credentials (e.g., passwords) to users and enables authentication using passwords

Best Practice – Get rid of them. If nothing else works, then use long, complex passwords that are frequently changed. But get rid of them wherever possible.

2.4.3. Authorization - Manages the granting of rights to a resource and determines whether access should be granted based on those rights

Best Practice – Authorization decisions should be driven by machine encoded policies rather than by managing explicit permission. Components of these systems need to include policy decision engines or PDPs (Policy Decision Points), PEPs (Policy enforcement Points) or accessible enforcement mechanisms in software and hardware, a way to manage the policies – typically called a PAP or Policy Administration Point, meta data about data and resources, meta data about principles or end users, and an auditing function. Individual components are described below. Standards describing this general architecture include ISO 10181-3, The Open Group XDSF and the IETF AAA RFCs. Standard protocols include LDAP, SAML, and XACML. A mature environment built on this architecture allows fine grained, policy based access control over resources within an enterprise – and if products are standards based even between enterprises, this would be a major contribution to supply chain security.

Standard – the recommended standard for Authorization is the OASIS XACML eXtended Access Control Markup Language. While SAML can do basic authorization, most of that functionality went into XACML 2.0. LDAP is used to supply meta information to policy decision points – it is not an authorization protocol per se.

The following Access Control Principles from the Open Group Jericho Forum are relevant to creating good authorization architectures:

9. A resource owner must define Entitlement (Resource Access Rules).

Resource owners define rules and trust levels for access to their resources. Notes: Current systems are often too inflexible, especially those that operate between enterprises. Authorization products are often proprietary rather than using standard protocols. Applications that manage resources seldom externalize their authorization decisions.

10. Access decisions must be relevant, valid and bi-directional.

Attributes and access control rules determine access to resources. Attribute Derivation should be used where possible to limit attribute exposure. Notes: Many authorization systems collect more identity information than necessary – simply because it's easier to be global. Attribute Derivation is relatively rare.

11. Users of an entity's attributes are accountable for protecting the attributes.

Relying parties and resource owners are responsible for protecting attributes they collect for making access decisions. Attributes should be destroyed when no longer needed. Note: Attributes tend to accumulate, making them a rich target for identity theft and other acts against the entities they represent.

12. Principals can delegate authority to another to act on behalf of a persona.

An Entity must be able to delegate resources it owns to another entity or principal. Notes**:** Many delegation systems rely on impersonation. Delegation without impersonation along with careful audit records should be encouraged.

13. Authorized Principals may acquire access to (seize) another entity's persona.

This is to support the ability to freeze the actions of a rogue Identity. And to recover access assets controlled by a rogue Identity. Notes: Emergency access to and control of an Identity's resources must be carefully constrained and logged. Legal actions to stop a rogue Identity should not lead to impersonation.

14. A persona may represent, or be represented by, more than one entity.

This is intended to provide support for class identities such as Groups and Roles. Note: Many mechanisms, particularly PKI, do not support delegation without impersonation.

Best Practice - Maintain appropriate access regardless of where the resource is located.

Best Practice - Externalize authorization capabilities from targets.

Best Practice – The following design principles should be used for creating policy driven access control systems:

- **Policy Driven** – Policy, regulations, and business rules directly drive access decisions.
- **Automated** - Access decision and enforcement is automatic.
- **Disintermediated** – Access control services are built using separate, loosely coupled components. Scalability requires that PEPs be distributed and placed close to the resource being protected, while PDPs are often an enterprise wide service.
- **Standardized** – Access control services use a common set of standard interfaces and protocols to decide, communicate, and record access.
- **Integrated** – Access control services use common administration, accounting and auditing services.

2.4.3.1. Account & Access Management - Creates accounts (e.g., end user, privileged, administrator) and privileges, associates these accounts and privileges with the appropriate identity, and manages the accounts and access throughout the lifecycle of the user

Best Practice - Provision accounts and access to a few, strategic repositories rather than trying to provision to every application. This centralizes account management and auditing, reduces the possibility of errors, lowers the attack surface and helps an organization understand where its trust flows go. Standards for account management would be useful here.

2.4.3.2. Federated Authentication - Enables authorization decisions by using identity data that is managed within another security domain (e.g., granting access to SWA maintenance data via an assertion from SWA claiming Joe is part of the maintenance team)
Practice Gap – Other than assertion of roles commonly defined among organizations collaborating on support of a critical infrastructure, Federated Authorization depends on propagating access control policies from the relying organization to the asserting organization with assurance that those policies will be adhered to. There is currently no really viable approach to implementing this except where a general scope of access is allocated to the asserting organization with the expectation that they can control specific access requests within that scope as they see fit.

2.4.3.3. Level of Assurance - Determines the strength of an authentication event by evaluating several factors (e.g., type of authenticator, trust level of authentication service) for use during an access decision
Best Practice – The level of authentication assurance should be one factor taken into account when making an access decision. Cooperative enterprises need to establish level of assurance rules for shared data. There are several current practices, but the most widely recognized one is contained in NIST 800-63.
Best Practice - Virtual machines can be configured to require keys to boot and to decrypt their data partitions. Example – the Safenet KeySecure appliance and their VProtect software. The VM must speak to the HSM and get its keys at boot time, so the entire VM cannot be copied and run elsewhere.
Best Practice - Crypto as a Service – we are trying to provide HSMs for apps with critical needs – signing keys, or those that want higher server identity assurance.

2.4.3.4. Policy Administration - Creates and manages the access policies used to protect access to a resource which specify the rules (e.g., US Persons only, Finance department only) under which access is allowed
Best Practice – As resource and data protection transitions to policy controlled systems, the role of the administrator becomes critical. Policy administration points are used to create and map attributes into access policies. These administrative interfaces need to be highly secure. If an attacker can't break the protection mechanisms the attacker will go after the user's identities and those services that map identities to access.
Best Practice - Manage policies once… distribute them where they need to be enforced.

2.4.3.5. Policy Decision - Determines whether the operation on a specific resource by a specific user is authorized by using data about the user, resource, and environment and comparing it against the rules specified in the access policy
***Best Practice* -** Access Control systems should handle both static and dynamic attributes. For internal access control systems, provision and enroll as much as possible and use dynamic access control for ad-hoc or exception situations. Dynamic access control systems allow enterprises to share resources without requiring local accounts.
Best Practice - Ensure users are only able to access data and resources that are necessary for a legitimate purpose by granting access that is in compliance with policy and satisfies need to know.
Best Practice - Centralize policy decision points without introducing latency or performance bottlenecks.

Best Practice – When making a decision authorization services should consider:

- The Principal the Identity represents
- The Identifier to attribute binding strength
- The Attributes themselves
- The environment of the Principal
- The risk of the requested action against the Resource
- The value of the Resource
- Constraints imposed on access to the Resource
- The strength of the Access Control system itself

2.4.3.6. Policy Distribution - Provides access to access policies required by a policy decision point to make accurate access decisions
Best Practice – Policy distribution points need to be highly available and reliable. Once an enterprise transitions to policy based access control, failure of the Policy Decision service will result in denial of service to those resources governed by the service. Policy distribution points allow for scalability and fail over for the decision services.

2.4.3.7. Policy Enforcement - Ensures access decisions made by a policy decision point are enforced (e.g., grant or deny access) and ensures that any obligations are fulfilled (e.g., label/tag data, log access)

Best Practice - Secure solutions to the greatest possible degree by layering security controls. Ideally these would be different types of controls. For example, encryption at the data layer, login at the application layer and port filtering at the network layer.

Best Practice - Move policy enforcement points as close as possible to the target they are protecting

2.4.3.8. Audit Log Capability – Ensures that all access is documented. Protect audit logs from tampering.
Best Practice – All access should be logged. Access failures should also be logs. The logs need to be protected.

Best Practice - Create and store logs separately from the target that is generating the log data.
Best Practice - Encrypt logs containing sensitive data.

2.4.4. Directory Services - Stores and publishes security data required for authentication and authorization.

2.4.4.1. Data Management - Manages security data (e.g., identities, accounts, entitlements) used for identification, authentication, or authorization

2.4.4.1.1. **Database** - Identifies the appropriate use, architecture, and implementation of databases to manage, store, and provide access to security data

Best Practices:

- Architect with high availability product (N-way multi-master replication for LDAP repositories, clustered database servers with automated failover), deploy in multiple geographic regions with load balancer for local and global traffic management.
- Features of databases make them better suited to data management
- Features of directory services make them better suited to high-volume rapid authentication, authorization, and lookup of single entities (or small sets of entities).
- Manage data in a database, publish in LDAP directory.
- Publish in enterprise directory for data that is required by wide range of applications.
- Publish in special purpose directories to meet the specific needs for applications or customers (i.e. Windows, Unix Authentication, segregated directory for customer environment, network segmentation, classified environment).
- Perform centralized identity data management where no better service is available. Although in principle we wish to "own" as little data as possible, some data still makes sense to manage centrally
- Externalize authentication and authorization mechanisms to centralized administration.
- Prevent data spill, limit/control access so that consumers have access only data that is necessary for their business.
- No direct access to backend servers, utilize virtual directories/directory proxy to serve as the interface for direct data access.

2.4.4.1.2. **Data Sources** - Identifies the appropriate use, architecture, and implementation of data sources outside of Information Security used to supplement security data managed within Information Security
Best Practices:

- We should “own” as little information as possible, aggregate information from other authoritative sources.

- Consider gathering identities from external identity providers.
- Consider publishing and subscribe service for getting identity attributes (e.g., US Person Status, Denied Person Lists).
- Document interface agreements for data availability and reliability.

2.4.4.1.3. **Meta Directory** - Identifies the appropriate use, architecture, and implementation of meta-directories to manage, store, and provide access to security data

Best Practices:

- Collect data from authoritative sources only.
- Provide standard access to publishing authorities.
- If using custom code for aggregation for each data source, consider standardization; make it repeatable or re-useable for aggregating new data sources.

2.4.4.1.4. **Synchronization** - Coordinates data changes to apply data transactions in the correct order and to avoid unexpected race conditions

Best Practices:

- Many applications require their own user identity store. Synchronization enables such applications to be managed more efficiently by obviating the need to redundantly manage identity data in the proprietary user identity store.
- Synchronize only data that is needed for the apps.

2.4.4.2. **Data Publication** - Provides access to security data (e.g., identities, accounts, entitlements) used for identification, authentication, or authorization through the use of enterprise information points (e.g., Enterprise Directory Services)

2.4.4.2.1. **Directory Proxy** - Provides a decoupled interface to databases or meta-directories and provides performance management, data mapping, data transformation, load balancing, and failover capabilities

Best Practice - Clients shouldn't have direct access to the underlying data store. We should support API and direct protocol (e.g., LDAP) access to the data we publish and get rid of flat files that we send to systems.

Best Practices:

- Setup client connection policies for fine grained traffic management.
- Use enhance health checks (e.g., direct traffic to other servers if replication is backlogged or server is busy)
- Use load balancer for local and global traffic management.

2.4.4.2.2. **Formatting** - Transforms data from one state to an accepted stated before the data is published in a database or meta-directory

Best Practice – Flexibility. We should be able to transform and assemble little pieces of data as needed by relying applications.

Best Practices:

- Use industry standard format for publishing to data consumers.

- Have reusable/configurable routines for formatting data from data sources and data for publishing to endpoints.

2.4.4.2.3. **Protocols** - Identifies the protocols that are allowed and supported for clients attempting to access data published in a database or meta-directory

Best Practices & Standards:

- Use industry standard protocols for access to repositories
- Utilize LDAP/LDAPS as the protocol for direct data access.
- Utilize SOAP for programmatic access.
- Utilize SQLNET/NET8 for publishing data for database to applications.
- Consider using ReSTful API for programmatic data access.
- Mandate use of secure protocol(LDAPS, StartTLS)
-

2.4.4.2.4. **Replication** - Ensures data consistency between redundant resources (e.g., software, hardware) to improve reliability, fault-tolerance, or accessibility

Best Practices:

- Use directory product that supports N-way multi master replication.
- Use DB product that is fault tolerant with automatic failover
- Tune replication to reduce WAN traffic(e.g., compression or designate primary WAN replicator)

2.4.4.2.5. **Virtual Directory** - Provides a decoupled LDAP interface to databases or meta-directories and provides data mapping and data transformation capabilities

Best Practices:

- Decouple backend repositories from direct access by applications.
- “Hide” underlying data structures from applications so that changes or reorganization of structure don’t impact them.
- Use load balancer for local and global traffic management.
- Prevent data spill, limit/control access so that consumers have access only data that is necessary for their business.

2. 5. Intelligence Services – Provides analysis that enhances the decision-making process. The dissemination of the subsequent intelligence is the basis for decisions concerning the current and future threat and as such are the foundation for action

2.5.1. Information Gathering The process whereby information is collected and collated to form the basis of analysis.

2.5.1.1. Information Collaboration & Exchange - Ensures that adequate guidance is provided to personnel regarding Info Security in addition to providing a means to share ideas, approaches and experiences on the topics associated with Information Security

Best Practice - The collection process should be an all source model (to include internal log collection and machine reporting – some will be paid for subscription-based services) and Counter Intelligence against your company.
Best Practice - Segregate an intelligence network from the main network

Best Practice – The following are source of information that should be pursued – each have their advantages.

Government - Supports the method by which intelligence is obtained from government agencies in hopes of proactively preparing the enterprise for potential events. Government information is often restricted and cannot be retransmitted to business partner, customers, or suppliers.

Industry - Ensures there is adequate collaboration with peers throughout the industry to provide a means of self-assessing service offerings against industry standards. The best industry information is obtained via organizations that have strong NDAs to encourage sharing. Long term relationships build trust and enhance industry based sharing.

Subscription Services – Leverages the availability of commercial intelligence services that provide online alerts, newsletters and other notifications. Subscription services vary in quality, content and price. Good services are a useful supplement to other information sharing methods.

Security Conferences & Events - Provides a means of allowing personnel to be made aware of new technologies and emerging products in the areas associated with Information Security.

2.5.2. **Intelligence Reporting –** The product of the Intelligence process that is evaluated for decision-making

Best Practice - Maintain both intelligence analysts and cybersecurity engineers as a means of making connections faster.
Best Practice - Have a dedicated Cyber Intelligence organization that can provide enterprise wide distribution and analysis for executive level decision-making.
Best Practice - Establish a Request for Information (RFI) process to allow for high priority collection and analysis efforts.
Best Practice - Develop and maintain Intelligence Requirements

2.5.2.1. **Situational Reports & Threat Briefings –** Designed to highlight specific threats over a period of time

Best Practice - Standardize briefing formats for consistency and the ability to highlight salient points.
Best Practice - Develop a strategic intelligence plan that will guide decision-makers in all matters security related.
Best Practice - Publish situation reports and briefings to key decision makers on a regular basis.

2.5.2.2. **Threat Profile Reports -** An in-depth study of a specific threat actor

Best Practice – These can be useful when up to date or prepared for specific situations. They require significant collection or collateration capability, but that is getting easier with the wealth of open source information available on line. While much data is available on line, it takes skill to weed out useless information and compile actionable reports.

2.5.3. Vulnerability Assessments - Supports the processes and procedures which facilitate the identifying, quantifying and prioritizing of threat vectors associated with a network, system or site
Practice Gap – Consistent vulnerability assessment criteria and compliance levels are needed for any effective use of assessment results to be useful in establishing consistent security levels across a critical infrastructure and the organizations supporting it.

2.5.3.1. Assessments - Provides the means of quantifying the inherent security risks associated with a specific network, devices or sites
Best Practice- Use a formal, documented methodology that covers the external attack surface, internal networks, operating systems, and selected applications.
Best Practice – Document and categorize the findings (results), document potential remediation, and provide an executive summary.
Best Practice – Augment comprehensive assessments with targeted Red Team activities.

2.5.4. Monitoring & Threat Detection - Ensures a comprehensive understanding of the health, security, and stability of a system or system of systems by recording, correlating, and analyzing important events

Practice Gap – Consistent monitoring and threat detection criteria, data syntax and semantics, and compliance levels are needed for any effective use of monitoring and threat detection results to be useful in establishing consistent security levels across a critical infrastructure and the organizations supporting it.

Best Practices

- Standardize the method for defining and tracking events of interest.
- Identify supported logging techniques and formats.
- Identify supported event providers .
- Utilize a central collection mechanism for security events.
- Leverage industry products to correlate events from various sources.
- Develop rules for the automatic identification of trends.
- Develop reports that simplify the manual effort for refining the rules.
- Integrate security event analysis with standard enterprise alerting tools or dashboards
- Transform existing policy into a machine-enforceable format.
- Aggregate data from existing enterprise stores and compare against policy to identify compliance and non-compliance.
- Provide visibility of the actual impacts of not complying with policy.
- Provide tools which can perform “what-if” analysis of policy changes.

2.5.4.1. Analytics - Examines a correlated set of events so as to identify root cause, key factors, possible results, and patterns

Best Practice – Employ heuristics-based analytic software to mine event logs from disparate systems for patterns which may indicate a security event. Analytic tools must support real-time monitoring and alerting.

2.5.4.2. **Correlation** - Maps seemingly disparate events from various sources into an orderly, connected set of events that can be analyzed.
Best Practice – Employ heuristics-based event correlation software to parse large data sets from a wide variety of computing platforms and applications, determine commonalities between events and sources, and associate events for security incident handling. The output from correlation systems serves as input to analytic systems.

2.5.4.3. **Intrusion Detection** - Enables the use of processes and tools which are designed to identify and report on malicious activity.
Best Practice – Deploy intrusion detection systems across networks. Focus network deployment on perimeters and key application-hosting networks, if it is not possible to deploy to entire enterprise. Deploy intrusion detection agents to servers, focusing on key applications if it is not possible to deploy to all servers. Intrusion detection systems should be fine-tuned to reduce false positives. Logs from intrusion detection systems should be sent to correlation and analytics engines for ongoing analysis.

2.5.4.4. **Intrusion Prevention** - Enables the use of processes and tools which are designed to minimize the associated impacts of any potentially malicious events.
Best Practice – Deploy intrusion prevention systems (IPS) across networks. Focus network deployment on perimeters and key application-hosting networks, if it is not possible to deploy to entire enterprise. Deploy intrusion prevention agents to servers, focusing on key applications if it is not possible to deploy to all servers. Intrusion detection systems should be fine-tuned to reduce false positives. Most IPS tools can actively interdict suspicious actions and traffic. Use of these capabilities is encouraged, and administrators must exercise caution in deployment so as not to impede legitimate actions and traffic. Logs from intrusion detection systems should be sent to correlation and analytics engines for ongoing analysis.

2.5.4.5. **Logging** - Records key events that are important to determine system health, security posture, or impending issues by using a standard format and storage location.
Best Practice – Determine which types of log entries may indicate some level of a security event for each system to be monitored. Develop standard set of log entry / events / formats to capture. Utilize standard interfaces for sending endpoint, server, and network logs to centralized correlation engine.

2.5.4.6. **Reporting** - Provides an account or statement describing in detail a series of events and any observation or conclusions that can be drawn from analyzing these events.
Best Practice –Reports from correlation and analytics systems must be distributed to the appropriate personnel. Determine which groups need security incident reports

(Security Operation Center [SOC] staff, incident responders, and management) and set up distribution mechanisms to provide real-time reporting.
Best Practice - Establish communication protocols for incident response and post incident analysis. And test them.

2.5.4.7. Display – Provides a clear status indication of the enterprise health from a security perspective.
Best Practice –Output from correlation/analysis/reporting systems should be presented as a security dashboard for Security Operation Center [SOC] staff, incident responders, and management consumption. Display technologies should be resilient and capable of real-time updates.

2.5.5. Investigation and Response - Specifies that adequate processes, tools, monitoring and defined remediation instructions are in place to facilitate the expeditious identification and handling of any malicious events

2.5.5.1. Attack Containment - Outlines, documents, and executes the steps necessary to minimize the impacts of any identified malicious activity

Best Practices --

- Develop and maintain attack profiles and thresholds of anomalous behaviors.
- Automatically quarantine devices suspected of compromise to low-risk environments.
- Automatically restrict credentials suspected of compromise to a minimal set of local entitlements.
- Leverage intrusion prevention and containment technologies that are built into security monitoring tools, for critical assets.
- Deploy Network Intrusion Detection/Prevention (NIDPS) systems at critical internal network segments (i.e. Enclave ingress/egress points).
- Develop a stand-alone NIDPS for rapid deployment.
- Maintain separation of classified data from non-classified data

2.5.5.2. Forensics - Examines digital information with the aim of identifying, preserving, recovering, analyzing, and presenting facts and opinions about events such as employee misconduct, product accident investigations and civil litigation.

Best Practices -

- Develop ways to immediately access trained/credentialed forensics examiners (internal or external contract) to support internal investigations.

- Create and document internal investigation and legal response processes and technical methods that include the definition of how to discover, collect, preserve and examine digital evidence/artifacts from across the enterprise systems.

- Define system/log alerts that identify potential abuse/misuse of enterprise systems.

2.5.5.3. Root Cause Analysis - Identifies the use of a structured approach in identifying factors that contributed to events which resulted in negative outcomes for the business

Best Practices -

- Use technical structured methods and tools to capture cause and effect. For example: Force Field Analysis; Gap-to-Goal Analysis; 4-Square (High Level Summary; Cause & Effect (Fish Bone) Diagrams; 5-Whys Analysis; FMEA (Failure Mode & Effect Analysis); Process Flow Charts; Precedence Diagram & Critical Path; Defect Locator ('Measles') Charts

- Sponsor, at the appropriate executive level, and create root cause processes to include all key knowledge holders during root cause investigations.

2.6. Resiliency Services - Ensures that an enterprise is capable of performing its mission under adverse conditions. These may be caused by natural events or overt attacks

2.6.1. Load Balancing – Critical services are replicated and load balanced to ensure that they are available

Best Practice - Use different switches for the primary and failover network interfaces

2.6.2. DDOS Protection – Technical capability is deployed to prevent Distributed Denial of Service (DDOS) attacks from interfering with an organization's ability to conduct business over the Internet.

Best Practice – Many Internet Service Providers (ISPs) provide a service to identify DDOS attack patterns and block such traffic deeper within their network so as to reduce impact on "last mile" capacity to their customers.

2.6.3. Contingency and Disaster Planning - Ensures that systems have outlined, rehearsed, and documented all the necessary steps that would be required in the wake of a catastrophic event including archival, backup, and recovery

Best Practice – Conduct exercise to simulate disasters and modify business continuity capability based on the results. It seems obvious, but this is rarely done.

END