U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

NHTSA
www.nhtsa.gov

DOT HS 812 075

October 2014

A Summary of Cybersecurity Best Practices

DISCLAIMER

This publication is distributed by the U.S. Department of Transportation, National Highway Traffic Safety Administration, in the interest of information exchange. The opinions, findings, and conclusions expressed in this publication are those of the authors and not necessarily those of the Department of Transportation or the National Highway Traffic Safety Administration. The United States Government assumes no liability for its contents or use thereof. If trade or manufacturers' names or products are mentioned, it is because they are considered essential to the object of the publication and should not be construed as an endorsement. The United States Government does not endorse products or manufacturers.

Suggested APA Format Citation:

McCarthy, C., Harnett, K., & Carter, A.. (2014, October). *A summary of cybersecurity best practices.* (Report No. DOT HS 812 075). Washington, DC: National Highway Traffic Safety Administration.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
DOT HS 812 075		

4. Title and Subtitle	5. Report Date
A Summary of Cybersecurity Best Practices	October 2014
	6. Performing Organization

7. Author(s)	8. Performing Organization
Charlie McCarthy, Kevin Harnett, Art Carter	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Volpe National Transportation Systems Center Security and Emergency Management Division 55 Broad Street Cambridge, MA	11. Contract or Grant No. DTNH22-12-V-00085 DTFH61-12-V00021

12. Sponsoring Agency Name and Address	13. Type of Report and Period
National Highway Traffic Safety Administration Office of Program Development and Delivery 1200 New Jersey Avenue SE. Washington, DC 20590	Final Report 14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report contains the results and analysis of a review of best practices and observations in the field of cybersecurity involving electronic control systems across a variety of industry segments where the safety-of-life is concerned. This research provides relevant benchmarks that are essential to making strategic decisions over the next steps for NHTSA's research program.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

17. Key Words	18. Distribution Statement
Cybersecurity, NIST, NHTSA, Guidelines, Risk Management, Baseline, Use cases, Best Practices	Document is available to the public from the National Technical Information Service www.ntis.gov

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22
Unclassified		40	

Form DOT F 1700.7 (8-72) Reproduction of completed page authorized

Foreword

NHTSA's Automotive Cybersecurity Research Program

Based on a systems engineering approach, the National Highway Traffic Safety Administration established five research goals to address cybersecurity issues associated with the secure operation of motor vehicles equipped with advanced electronic control systems. This program covers various safety-critical applications deployed on current generation vehicles, as well as those envisioned on future vehicles that may feature more advanced forms of automation and connectivity. These goals are:

1. Build a knowledge base to establish comprehensive research plans for automotive cybersecurity and develop enabling tools for applied research in this area;
2. Facilitate the implementation of effective, industry-based best practices and voluntary standards for cybersecurity and cybersecurity information-sharing forums;
3. Foster the development of new system solutions for automotive cybersecurity;
4. Research the feasibility of developing minimum performance requirements for automotive cybersecurity; and
5. Gather foundational research data and facts to inform potential future Federal policy and regulatory decision activities.

This report

This report contains the results and analysis of a review of best practices and observations in the field of cybersecurity involving electronic control systems across a variety of industry segments. This research provides relevant benchmarks that are informative to making strategic decisions for NHTSA's research program.

This publication is part of a series of reports that describe our initial work under the goal of facilitating cybersecurity best practices in the automotive industry (Goals 1 and 2). The information presented herein increase the collective knowledge base in automotive cybersecurity; help identify potential knowledge gaps; help describe the risk and threat environments; and help support follow-on tasks that could be used to establish security guidelines.

Table of Contents

1 Executive Summary

1.1 Background

The National Highway Traffic Safety Administration performed a review of cybersecurity best practices and lessons learned in the area of safety-critical electronic control systems. This review was across a variety of industries in which electronic control systems are used in applications where breaches in cybersecurity could impinge on critical control functions and therefore could jeopardize safety of life.

1.2 Cybersecurity Research Methodology

This research targeted cybersecurity best practices used in non-transportation industries and in other transportation modes. It was important to summarize from the experience (both successes and failures) of government and private sector professionals who have been developing cybersecurity strategies, policies, and approaches. By looking outside the automobile industry, and indeed outside the transportation industry itself, the goal was to understand the potential key elements of a cybersecurity program.

The focus of the research was to examine industries with commonalities to the auto industry with respect to cybersecurity, and to study the state of these industries' efforts to understand their cybersecurity issues and how they are improving their cybersecurity posture. The specific objectives were to bring forward key observations to help NHTSA craft a strategic roadmap for cybersecurity.

Government and industries studied were:

- Information technology and telecommunications,
- Industrial control systems and energy,
- Medical devices,
- Aviation,
- Financial payments, and
- National Institute of Standards and Technology (NIST).

Research consisted of three steps:

1. Literature study of relevant cybersecurity research, guidelines, best practices, and standards in target industries;
2. Issuance of a Request for Information (RFI) to obtain informed views on the perceived needs, prevailing practices, and lessons learned concerning the cybersecurity and safety of safety-critical electronic control systems used in various modes of transportation and other industry sectors; and
3. Interviews with subject matter experts (SME).

1.3 Findings

The information technology (IT) industry is a good model for cybersecurity protection based on its experience, exposure to, and addressing of issues. The telecommunications industry helped accelerate the advancement of hacking activities and exposing key systems (hardware and software) by advancing networking and enabling the development of the Internet.

The IT security industry developed best practices over the years that include the basic tenet that information security is a life-cycle process.

While all the elements of a Life-Cycle Risk Management Program are important, perhaps the most vital element of any cybersecurity program is to perform risk assessments on all systems, sub-systems, and devices to determine what vulnerabilities are present.

It is important that the risk analyses identify and quantify the consequences of risks. A very effective methodology for risk assessment is the development of use case scenarios. Proper cybersecurity threat modeling can help create a better and more effective risk mitigation plan through:

- Emphasis on asset management and risk reduction before acquisition of information and security technologies;
- Selection of correct countermeasures; and
- Justification of investments in security, compliance and risk management.

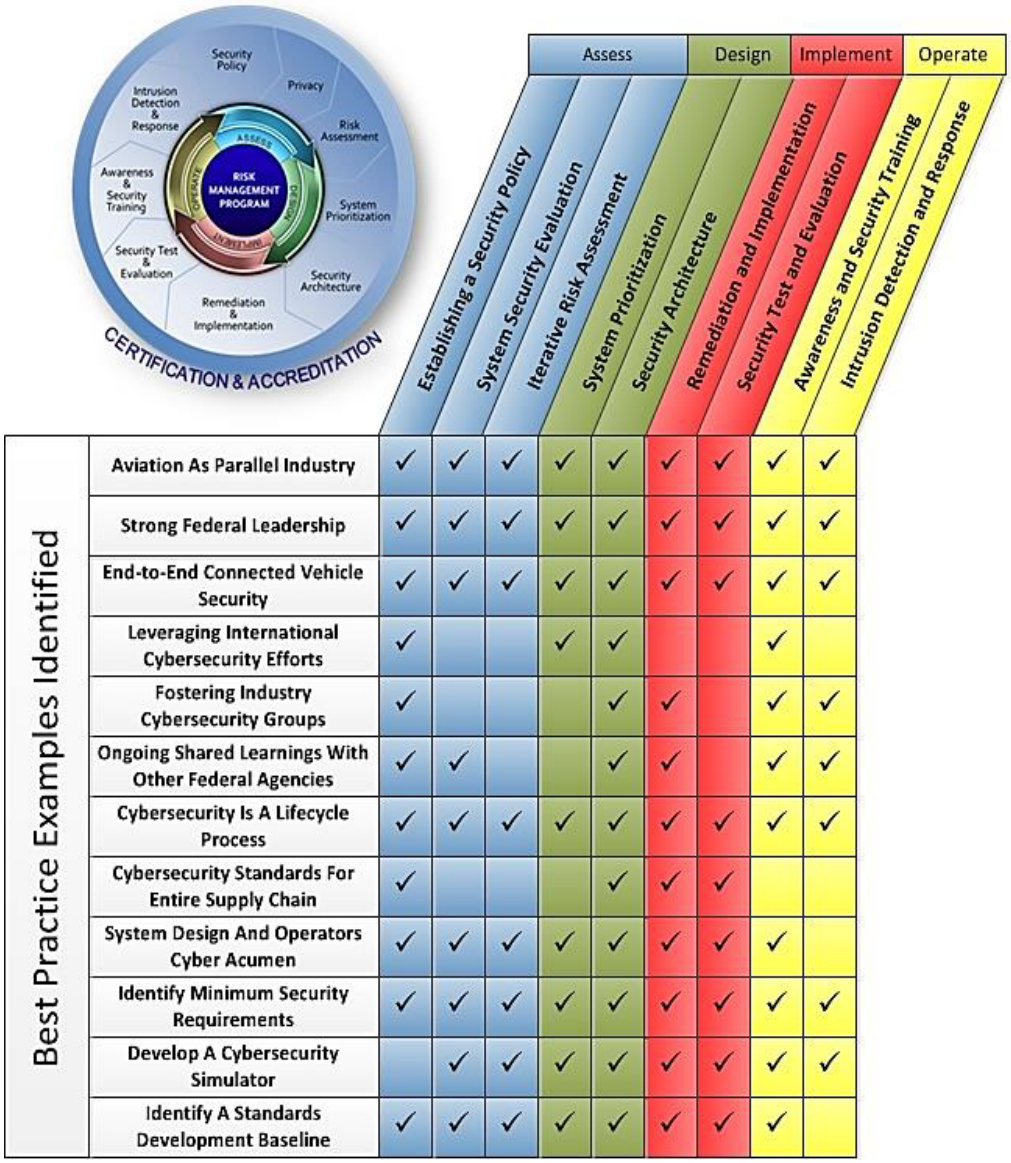
Individual industries examine the best practices of this life-cycle approach and create industry-specific security guidelines that address the need for robust risk management that includes the assessment, design, implementation, and operation phases of critical systems.

The research of the various industries studied has yielded some example best practices, shown in the following table.

Key Observation	***Source***
Cybersecurity is a life-cycle process that includes elements of assessment, design, implementation, and operations as well as an effective testing and certification program	All
The aviation industry has many parallels to the automotive industry in the area of cybersecurity	FAA
Strong leadership from the Federal Government could help the development of industry-specific cybersecurity standards, guidelines, and best practices	FAA
Ongoing shared learning with other Federal Government agencies is beneficial	FAA, NRC, NIST
Use of the NIST cybersecurity standards as a baseline is a way to accelerate development of industry-specific cybersecurity guidelines	FAA, NIST, NRC, Automotive
International cybersecurity efforts are a key source of information	Automotive, Aviation
Consider developing a cybersecurity simulator. It could facilitate identification of vulnerabilities and risk mitigation strategies and can be used for collaborative learning (government, academia, private sector,	FAA

international)	
Cybersecurity standards for the entire supply chain are important	Automotive, Financial Payments
Foster industry cybersecurity groups for exchange of cybersecurity information	IT, DHS, NIST
Use professional capacity building to address develop cybersecurity skillsets system designers and engineers	All
Connected vehicle security should be end-to-end; vehicles, infrastructure, and V2X communication should all be secure.	Aviation, Automotive (EVITA)

Mapping these key observations to the process of a lifecycle information security program yields the stages in which each falls. This is shown in the figure below.



2 Study Findings

2.1 Background

NHTSA performed a review of cybersecurity best practices and lessons learned in the area of safety-critical electronic control systems. This review was across a variety of industries in which electronic control systems are used in applications where breaches in cybersecurity could impinge on critical control functions and therefore could jeopardize safety of life.

2.2 Cybersecurity Research Methodology

The research targeted cybersecurity best practices used in non-transportation industries and in other transportation modes. It was important to summarize from the experience (both successes and failures) of government and private sector professionals who have been developing cybersecurity strategies, policies, and approaches. By looking outside the automobile industry, and outside the transportation industry itself, the goal is to understand the potential key elements of a cybersecurity program.

The focus of the research was to examine industries with commonalities to the auto industry with respect to cybersecurity, and to study the state of these industries' efforts understanding their cybersecurity issues and how they are improving their cybersecurity posture.

Industries for the study were determined by examining, at a high level, whether industries have similar concerns, risks, and constraints to that of the automobile industry; either similarity of the industry's use case or common issues or problem areas with respect to cybersecurity.

The research was performed in several steps. The first step entailed a literature study of relevant cybersecurity research, standards, guidelines, and best practices as well as forward-looking examinations of the growing need for cybersecurity in the use of information technology and wireless communications in cyber-physical (and especially safety-critical) systems.

Step two was the issuance of a Request For Information (RFI) to obtain informed views on the perceived needs, prevailing practices, and lessons learned concerning the cybersecurity and safety of safety-critical electronic control systems used in various modes of transportation and other industry sectors.[i]

This RFI yielded 13 responses from a cross section of private sector companies, industry consortia, and standards development organizations.

The third and final research step was to interview subject matter experts. The SMEs were chosen by examining the findings of the literature study and RFI, as well as through interactions with members of industry.

2.2.1 Industries Studied

Table 1 summarizes the industries studied and the rationale for their inclusion.

Table 1: Industries Studied and Why

Industry Studied	Why Studied
Information Technology	The IT industry has developed some of the more current best practices for addressing cybersecurity.
Telecommunications	IT Systems (and now cyber-physical systems, including control systems on automobiles) are connected through various wired and wireless communications protocols. The Internet, cloud computing, etc. has led to: • Increased threat vectors of the hacking community, and • More sophisticated hacking (online shared tools and hacking social networks, etc.).
Aviation	"Aircraft-airspace" is very similar to "vehicle-roadway" and the advent of NextGen parallels the vehicle-to-vehicle program somewhat. Additionally, eEnabled aircraft mirror today's vehicles. FAA has been working on security issues for several years.
Industrial Control Systems and Energy	Operational systems have been migrated using IT and mesh communications[1] but security is only now being addressed. • Infrastructure (networks/devices) often located in public spaces • Department of Homeland Security (ICS) and Federal Energy Regulatory Commission/Nuclear Regulatory Commission (energy sector) have been addressing the security issue for some time
National Institute of Standards and Technology	NIST is a Federal Government Standards Development Organization. Federal Information Processing Publication 199 *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) and NIST Special Publication 800 Series provide the baseline for Federal cybersecurity best practices, as well as a foundation for industry-specific security guidelines.
Financial Payments	A highly distributed risk (merchants, online storefronts, etc.) in the financial payments industry drives requirements to secure networks outside of the card issuers' purview.
Medical Devices	This includes the safety of life devices and systems. The industry requires a high degree of protecting individual privacy.
Automobile	Cybersecurity work is beginning in the U.S. marketplace. That work is leveraging international work. SAE International created the Vehicle Electrical System Security Committee. This group is gaining insight into the state of the industry with respect to cybersecurity.

These industries were studied using the three-step method discussed above. An initial literature research gave a general sense of each industry's cybersecurity issues and the methodologies used to address them.

No industry studied had a "solution" to cybersecurity. Rather, issues were actively being worked and methodologies being developed along the lines of what could generically be called the best practices of cybersecurity. These best practices are not, as might be assumed, technical fixes to observed vulnerabilities. Rather, the foundation of a cybersecurity program entails an iterative cybersecurity process over the entire life cycle of systems, sub-systems, software applications, or devices/hardware.

[1] Mesh Communications is a type of communications network topology where each node in the network must not only capture and disseminate its own data, but also serve as a relay for other nodes, that is, it must collaborate to propagate the data in the network.

2.3 Findings

2.3.1Information Technology and Telecommunications

The IT industry is has the most experience with cybersecurity issues. Initially academia turned to hacking into systems to do backdoor patching and testing, and more creatively for things such as making free telephone calls. Techniques and motives rapidly evolved as the IT world itself exponentially grew. Rapid development and evolution of telecommunications fed this exponential growth.

Telecommunications has based the entirety of its industry on the technologies, standards, services, and infrastructure established by IT. The telecommunications industry has been and continues to be coupled with that IT foundation to expand and facilitate services enabling the exchange of digital information. The business and technical issues of telecommunication are a very close parallel to the IT industry as a whole. The key differentiation is that telecommunications is the enabling set of services that enlist IT technology to provide services to all the industries that we are investigating.

This is an important factor to consider since wireless services are used for services relevant to the automotive industry such as toll collection systems, automated crash notification (ACN), vehicle-to-vehicle exchanges, and infotainment systems. This industry is what has enabled all the backroom operation services to be possible, and has delivered the conveyer of data asset exchange services in use today - the Internet. Telecommunications and the Internet have allowed hackers to form online communities to exchange ideas, tips, and hacking tools with targets being data.

Given these realities, the IT industry developed cybersecurity best practices over the years that include the basic tenet that Information Security is a life cycle process. Figure 1 shows the Information Security Program as an iterative life cycle.

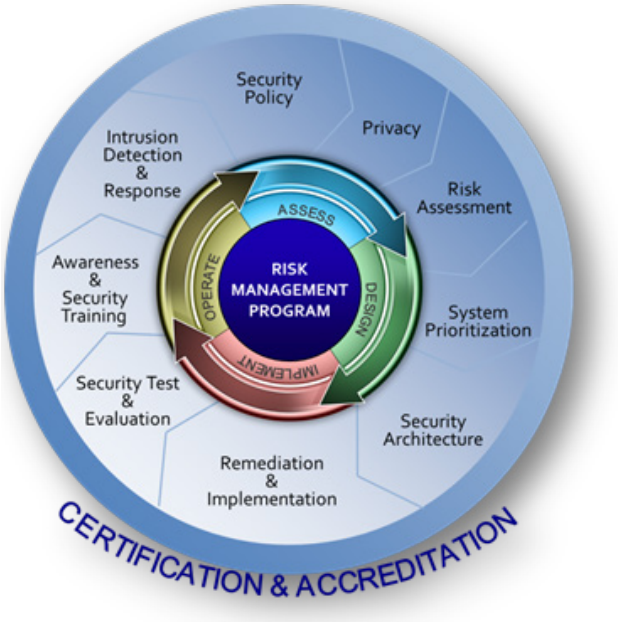


Figure 1: Information Security Life Cycle

While all the elements of the Life Cycle Risk Management Program are important, perhaps the most vital element of any cybersecurity program is to perform risk assessments on all systems, sub-systems, and devices to determine what vulnerabilities are present. This process is important for organizations as it is used to discover and categorize the security issues in their systems. It is also important that risk analyses identify and quantify the consequences of risk factors in applicable use case scenarios. Risk Assessment helps create a better and more effective risk mitigation plan because it:

- Emphasizes the focus on asset management and risk reduction before acquisition of information and security technologies.
- Is instrumental in selecting the right countermeasures often prioritizing monitoring before active data loss prevention (as an example)
- Justifies investments in security, compliance, and risk management

Detailed breakdowns of the Information Security Lifecycle elements are shown in Table 2 below.

Table 2: Details of the Information Security Life Cycle Process

Assessment Phase	
Establishing a Security Policy	A security policy includes administrative requirements and procedures in all the areas detailed below. Cybersecurity is beginning to be viewed as a need throughout organizations, not just in the IT area. Therefore there is a realization that cybersecurity should be championed not by the chief information officer, but rather the chief executive officer. All functional areas in an organization, from operations to human resources to IT, should play an active role in developing a robust security policy.
System Security Evaluation	Systems should be examined and evaluated for their security needs using established standards and best practices throughout their life cycle to uncover potential vulnerabilities. A sample standard document is the FIPS 199 Standards for Security Categorization of Federal Information and Information Systems.
Iterative Risk Assessment	Risks are measured through evaluation of the probability of the vulnerability being exploited as well as the severity to the system, organization, public, etc. if the system is compromised. A best practice document in this area for Federal IT Systems is the NIST SP 800.37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.
Design Phase	
System Prioritization	Once the risks have been identified and rated, they must be prioritized based on the organization's ability to apply appropriate resources (funding, technical skill sets, etc.) to address them in the most efficient manner.
Security Architecture	Examination of a system's security architecture is the final piece to the assessment of system security and the beginning of addressing vulnerabilities identified in the assessment phase.

Table 2: Details of the Information Security Lifecycle Process (Continued)

Implementation Phase	
Remediation and Implementation	Now that vulnerabilities have been identified, rated, and a security architecture developed, the findings should be implemented with appropriate security controls. Included in the implementation is a process for identifying the remediation of the fallout from potential exploitations of vulnerabilities. The Federal government guideline for developing the implementation and remediation plan is the NIST SP 800.53B *Recommended Security Controls for Federal Information Systems and Organizations*.
Security Test and Evaluation	A robust conformance testing and certification plan is vital to ensuring that appropriate security controls are compliant with security performance specifications. Once security controls have been applied and implemented in field systems, it is vital to continuously monitor the systems to ensure that any new vulnerabilities are identified and circumvented. An example of a best practice identified for this phase is FAA, which uses the Airborne Network Simulator System (ANSS) to attempt to exploit vulnerabilities in a controlled environment and evaluate potential consequences; so-called "white hat" hacking is intended to improve security measures.
Operation Phase	
Awareness and Security Training	Once fielded systems are in operation comes the need for ongoing training both to raise the awareness of the entire workforce of information security, but also to train specific users of systems in their appropriate, secure use. Often shortcuts are taken in the day-to-day operations of systems to save time and avoid procedures that users may deem "tedious" but are a vital means to keeping a strong system security posture.
Intrusion Detection and Response	The final phase is the ongoing monitoring of systems to identify attempted and successful exploitation of vulnerabilities. This constant monitoring is important in that it may yield vulnerabilities or attack vectors not previously thought of in the design and assessment phases.

2.3.2Aviation

Developing "eEnabled" Aircraft

About a decade ago, the potential for cybersecurity issues in new commercial aircraft and in the systems that communicate wirelessly between aircraft, airport ground equipment, and flight control systems began to emerge. Aircraft OEMs were developing "eEnabled technologies" that they were increasingly deploying into aircraft. The definition of eEnabled is any "device, system or combination of devices/components and systems that communicate with technologies other than point-to-point including interfaces between aircraft components and interfaces between aircraft and off-aircraft entities." Examples of eEnabled technologies include electronic flight bags (EFBs), WANs, cellular, Wi-Fi – 802.11b/g, and ethernet.

Legacy aircraft (e.g., B737, A320) have limited connections with external networks such as EFBs, Gatelink, and wireless LANs. However, eEnabled aircraft (e.g., B787, B747-8, A380, Bombardier C-Series) have many new and integrated external network connections (e.g., software data loading, broadband 802.11 connections, etc.) with airlines, airports, aircraft manufacturers, air navigation service providers, and repair organizations. The introduction of eEnabled technologies into new commercial aircraft is leading to unprecedented global connectivity that creates a new environment for the aviation sector. Aircraft navigation and communication functions are transitioning from operating as isolated and independent systems, to being integrated into a networked system that is dependent on exchanging digital information between the eEnabled aircraft and external networks located on the ground and on other eEnabled aircraft.

Due to the proliferation of these new connective technologies, it became necessary to re-examine security and safety of the aircraft to protect it against unwanted cyber intrusion. It would be essential to include cybersecurity within the certification criteria and processes.

Additionally, the cybersecurity approach of the new eEnabled aircraft should be coordinated with the move toward the Next Generation Air Traffic Control (NextGen) system. NextGen will evolve from a ground-based system of air traffic control to a satellite-based system of air traffic management which includes enhanced use of GPS and weather systems, as well as enhanced data networking and the use of digital communications. Security architectures and information sharing will be a vital element of this highly connected system, ensuring all system elements maintain appropriate levels of trust. This highly connected NextGen environment parallels the move toward Connected Vehicle systems and applications where automobiles and infrastructure will be connected.

Standards-Setting Efforts

In 2007, FAA engaged the Volpe Center to research and evaluate the requirements for airborne network security to ensure aircraft safety. The study required robust involvement from other government agencies (e.g., DHS and DoD), aircraft OEMs, suppliers, and academia. Because the cybersecurity of aircraft should be an international effort, the government of the United Kingdom was also involved. Activities of this study are delineated below.

Also in 2007, FAA helped lead the development of a standards development group in the Radio Technical Commission for Aeronautics (RTCA). This group (SC-216) developed the "Security Assurance and Assessment Processes for Safety-related Aircraft Systems" (DO-326). Published in December 2010, this "process" document is intended to augment current guidance for aircraft certification to handle the information security threat. It addresses only aircraft type certification but is intended as the first of a series of documents on aeronautical systems security that together will address information security for the overall Aeronautical Information System Security (AISS) of airborne systems with related ground systems and environment.

FAA has also staffed an internal national cybersecurity team to work on developing a standardized approach to address the cybersecurity vulnerabilities of aircraft equipment being installed during type certification, amended type certification, supplemental type certification, and field approval projects throughout the Aircraft Certification Service and Flight Standards Service.

Future work activities by the RTCA SC-216 group include examination and update of the FAA Instructions for Continued Airworthiness Order to address operational cybersecurity guidance for airline and maintenance repair organizations for eEnabled aircraft.

Cybersecurity Simulation Laboratory

In order to gain hands-on understanding and experience regarding how the various eEnabled components were integrated and what cybersecurity vulnerabilities may be present, FAA engaged the Volpe Center and Wichita State University (WSU) to develop the Airborne Network Security Simulator (ANSS). The goals for ANSS are to:

- Identify potential information security threats in a synthetic environment by simulating next generation aircraft communications systems;
- Share knowledge, tools, and methodologies with academia and other interested stakeholders to extend research value;
- Act as a coordinating authority for cybersecurity risk mitigation within the international aerospace & aviation community;
- Recommend appropriate technical & procedural standards for security risks to aid in the development of regulatory guidelines and policies; and
- Influence industry bodies on cybersecurity best practice with respect to specifications, procedures, and recommendations used by the industry.

Through these various activities, FAA has identified the following key areas requiring security controls.

- Electronic flight bags (EFBs)
- Gatelink
- Cellular
- Field loadable software
- User modifiable software
- Commercial off-the-shelf (COTS) equipment
- Integrated modular avionics
- Internal/external connectivity
- Wireless servers/routers
- Aviation sensors

Aircraft Certification Process and Issues

One of the key issues in the cybersecurity challenge for FAA is that, at this time, aircraft are not fully integrated with all of the eEnabled technologies and systems. This creates a difficult Type Certification (TC) and Supplemental Type Certification (STC) problem with respect to cybersecurity.

A different set of challenges may emerge as many of the legacy aircraft may be retrofitted with newer avionics as required to operate in a NextGen (U.S.) or Single European Sky ATM Research, SESAR (Europe) operational environment. Even older legacy aircraft will need to consider the importance of cybersecurity. Many scheduled for retrofit with the newer technology are subject to the same cybersecurity threats. This also increases complexity to the STC process by requiring a new security baseline for each aircraft model and subtype configuration.

The challenge will be how to properly mitigate and manage the installation and use of newer IP-enabled external networks, onto a legacy aircraft that was not originally designed to provide such capabilities. While the existing backplane has fewer capabilities for an external access to any part of the aircraft, previously isolated systems were never designed to protect or manage themselves while operating with some of the newer external access methods (SATCOM, wireless networks, etc.).

eEnabled Aircraft Technology Survey

In 2010, FAA and Volpe Center conducted a survey of aircraft OEMs, supply chain vendors, type certification inspection (DERs), and government/military organizations. The goal of the study was to gather information to be used to aid in future FAA planning related to regulations, directives, standards, guidance, training, and research regarding aircraft network security.

The survey results showed that the vast majority of respondents had aggressive plans for developing and adding eEnabled technologies into airframes: 63 percent of organizations planned to include eEnabled technologies and within three to five years and that number would grow to 83 percent. The inclusion of these technologies is a logical business decision for the aircraft manufacturers and the airlines. The business rationale includes:

1. *Weight savings*: no/less copper + less paper (i.e. EFBs) = fuel savings;
2. *Reduced labor cost*: for example, aircraft that are IP addressable allow mechanics remote access to the aircraft to perform maintenance; and
3. *In-flight entertainment*: provides a feature-rich environment for travelers and a revenue generator for airlines.

Supplemental Type Certification involving the incorporation of eEnabled technologies on legacy aircraft as well as the need to type certify new aircraft that are eEnabled will be a major workload for FAA in the next few years. Additionally, the survey findings show the need for eEnabled certification will expand by 63 to 83 percent over the next 5 years. This will influence FAA in the following areas:

1. FAA workload increases and workforce cybersecurity training increases;
2. OEM workload increases and workforce cybersecurity training increases;
3. Airline workload increases and workforce cybersecurity training increases;
4. Need for additional policy and rulemaking; and
5. Supply chain issues- need to ensure cybersecurity requirements are communicated and met by sub-tier vendors.

2.3.3Industrial Control Systems, Energy, and NIST

Connection between Industrial Control Systems, Energy, and NIST research

The ICS and energy sectors have been combined in this study due to the many similarities in the industries. In fact, ICS is not so much an industry as a type of system that is present in many industries. "Industrial Control Systems" is really a generic term that encompasses systems used to control industrial production, including Supervisory Control and Data Acquisition (SCADA) systems. However, the term is becoming more general and can be applied to systems that control operational activities. These control systems form a base for many infrastructures in industries including the energy sector. Therefore, the study of the energy sector paralleled the study of ICS.

NIST was combined with ICS and the energy sector since NIST creates many of the standards, guidelines, and best practices that are used for security standards for operational systems in each sector.

ICS can be used in the energy sector for controlling generation plant operations as well as to control the function of the power distribution network. The hallmark of ICS is that they are formerly closed and often proprietary systems that are electro-mechanical (cyber-physical systems) in nature. It is in this latter area that the research has concentrated in the energy sector due to the move toward Smart Grid.

ICS Research

Over the years, ICS has been increasingly enhanced with information technology hardware and software as well as increasingly connected via the Internet through a mesh network of wired and wireless communications. This migration has evolved ICS into distributed IT systems designed to enhance the operations of these formerly closed systems. While this migration has enhanced the performance of these systems, it has also introduced vulnerabilities.

A key standards document used in ICS is the NIST Special Publication 800.82 *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. This document is based on other NIST SP800 series documents but is specifically tailored for use in ICS and its unique use cases.

The Department of Homeland Security's Control Systems Security Program (CSSP) was created to examine vulnerabilities of these systems within the Nation's 18 Critical Infrastructure and Key Resource (CIKR) Sectors. Among these sectors are transportation, energy, and nuclear reactors, materials, and waste.

The DHS CSSP website, www.us-cert.gov/control_systems/index.html, is a key resource for background documents, tools, and best practices. In addition to connecting users with various best practices such as NIST standards and NIST Interagency or Internal Reports (NISTIRs), the CSSP connects ICS professionals and organizations with the ICS Cyber Emergency Response Team (CERT). A CERT is a key element in any industry cybersecurity program.

The Software Engineering Institute at Carnegie Mellon University developed the first CERT. In 2003, DHS collaborated with the institute to create the US-CERT, www.us-cert.gov/index.html. US-CERT acts as a resource for cybersecurity professionals to highlight cybersecurity incidents and provide support for incident response and forensic analysis as well as acts as a conduit for topical cybersecurity information. US-CERT has a robust warehouse of information products and alerts that are both technical and non-technical in nature. While US-CERT has widespread security information covering all IT security, the ICS CERT tailors its activities to the ICS world.

In addition to informational products and tools, the ICS CSSP provides hands on training- ranging from half-day awareness training to a one week technical course of study at the Idaho National Laboratory, as well as on-site resources to work one-on-one with operators to perform assessments of their systems.

DHS CSSP is also active in the support and facilitation of an ICS industry Information Sharing and Analysis Center (ISAC). ISACs are extremely valuable, cross-industry organizations that act as clearinghouses for information on cyber and physical threats, vulnerabilities, and solutions. They help members better understand their threats and vulnerabilities and are forums for anonymous submission regarding specific vulnerabilities and security breaches. Much more information on ISACs is available through the National Council of ISACs at www.isaccouncil.org/.

Another key element of ICS support is the ICS Joint Working Group (ICSJWG), which is a cross-industry group that includes the public and private sectors as well as academia, focused on reducing the risk to the nation's industrial control systems through information sharing throughout the 18 CIKRs. The ICSJWG facilitates cybersecurity knowledge sharing and provides tools, tips, and other informational products as well as administers a semi-annual conference to bring security professionals together.

Examining the ICS world beyond the involvement of DHS, there is a building understanding that control systems are no longer isolated, and therefore are no longer safe from the exploit of vulnerabilities.

The overarching key approaches in the ICS industry are:

- Proactive involvement of the Federal Government through DHS CSSP;
- Promotion of NIST standards, guidelines, and best practices;
- The establishment and active use of a CERT (government-sponsored) and an ISAC (industry consortium); and
- Industry outreach and training through exhaustive archives of informational products online and the management of the ICSJWG.

Energy (SmartGrid) Research

The electric power grid is evolving into a "smart grid" because of the demand for a more efficient and complex system that will allow the participants more control. The increase in complexity of the grid also increases the number of potential vulnerabilities in the system. These potential vulnerabilities to one of the United States' most vital national infrastructures led to the passing of the Energy and Independence Security Act (EISA) of 2007.

EISA assigns roles and responsibilities for various members of the Federal Government and the electric utilities industry and created two key organizations. The first is the Smart Grid Advisory Committee (SGAC), which is made up of private sector industry members. The mission of the SGAC is to "provide input to NIST on the Smart Grid standards, priorities and gaps, and on the overall direction, status and health of the Smart Grid implementation by the Smart Grid industry including identification of issues and needs and the Smart Grid Task Force" that consists of several Federal Government agencies. See www.nist.gov/smartgrid/committee.cfm.

The second group established by EISA is the Smart Grid Task Force, which is made up of 11 Federal agencies. The mission of the Task Force is to "ensure awareness, coordination and integration of the diverse activities of the Federal Government related to smart grid technologies, practices, and services." See www.ferc.gov/industries/electric/indus-act/smart-grid.asp.

Specific organizations called out by EISA are the Federal Energy Regulatory Commission (FERC) and NIST. FERC was earlier given authority to oversee the power grid when Congress passed the Energy Policy Act of 2005. EISA further tasks FERC "to adopt interoperability standards and protocols necessary to ensure smart-grid functionality and interoperability in the interstate transmission of electric power and in regional and wholesale electricity markets." See www.ferc.gov/industries/electric/indus-act/smart-grid.asp.

NIST was charged with developing guidelines on how to securely implement the smart grid systems. NIST states its goal in this work as "bringing together manufacturers, consumers, energy providers, and regulators to develop 'Interoperable standards'." See www.nist.gov/smartgrid/nistandsmartgrid.cfm.

NIST staffed its Smart Grid cybersecurity discipline area in order to facilitate the development of standards, guidelines, and best practices by members of the entire electric utilities industry. It should be noted however, that this level of activity on the part of NIST─ the creation of a SmartGrid standards working area led by a NIST Project Manager─ is not the norm. The reason for this level of activity is the mandate by EISA. When specifically asked how NHTSA may engage NIST in the creation of a similar

work are for electronic resiliency of automobiles, the NIST subject matter experts stated that they would do such a thing only if tasked by law. Therefore, this level of facilitation and leadership by NIST is not practical.

NIST Standards Developed

NIST has been a very active and successful steward of the development of standards for Smart Grid. Perhaps most noteworthy is the publication in August 2010 of NISTIR 7628 *Guidelines for Smart Grid Cybersecurity*. Volume 1 covers the *Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements*. This is a valuable guideline document for how to examine security in the Smart Grid, but may be equally useful as a baseline to follow for the automotive industry.

NISTIR 7628 Vol. 1 covers the following stages of the security approach.

1. Selection of Use Cases with Cybersecurity Considerations
2. Performance of a Risk Assessment
3. Setting Boundaries: The Beginnings of a Security Architecture
4. High Level Security Requirements
5. Smart Grid Conformity Testing and Certification

These are the same basic steps in the life cycle approach to information security discussed previously. This is not surprising since listed standards references include FIPS 199 and several of the NIST SP 800 series documents.

Other NIST accomplishments thus far include the identification of 75 initial standards—uniform ways of doing business that should be considered to make an interoperable, secure Smart Grid a reality. Additionally NIST has identified five "foundational standards" for consideration by federal and state regulators. The standards describe common data communications formats that would allow Smart Grid devices and networks to work seamlessly and that specify cybersecurity protocols.

The basic finding in the examination of Smart Grid is that development of standards, guidelines and best practices have been based on establishing the use of existing standards as baselines, then modifying them for the specific needs of Smart Grid. Armed with a basic set of guidelines individual vendors or operators can then craft technical solutions to meet minimum security requirements developed collaboratively, but led strongly by the Federal Government and industry regulators.

Nuclear Regulatory Commission

In the course of research efforts, the opportunity arose to learn about the inroads that the Nuclear Regulatory Commission (NRC) has undertaken regarding cybersecurity. The mission of the NRC is to enable the nation to safely use radioactive materials for beneficial civilian purposes while ensuring that people and the environment are protected. The NRC regulates commercial nuclear power plants and other uses of nuclear materials, such as in nuclear medicine, through licensing, inspection and enforcement of its requirements. See www.nrc.gov/about-nrc.html.

NRC has a very strict compliance infrastructure by nature of its mission. NRC's master regulatory guidance comes from Chapter 1 of Title 10, "Energy," of the Code of Federal Regulations (CFR). Chapter 1 is divided into Parts 1 through 199. NRC's regulatory practice is highlighted in Figure 2.

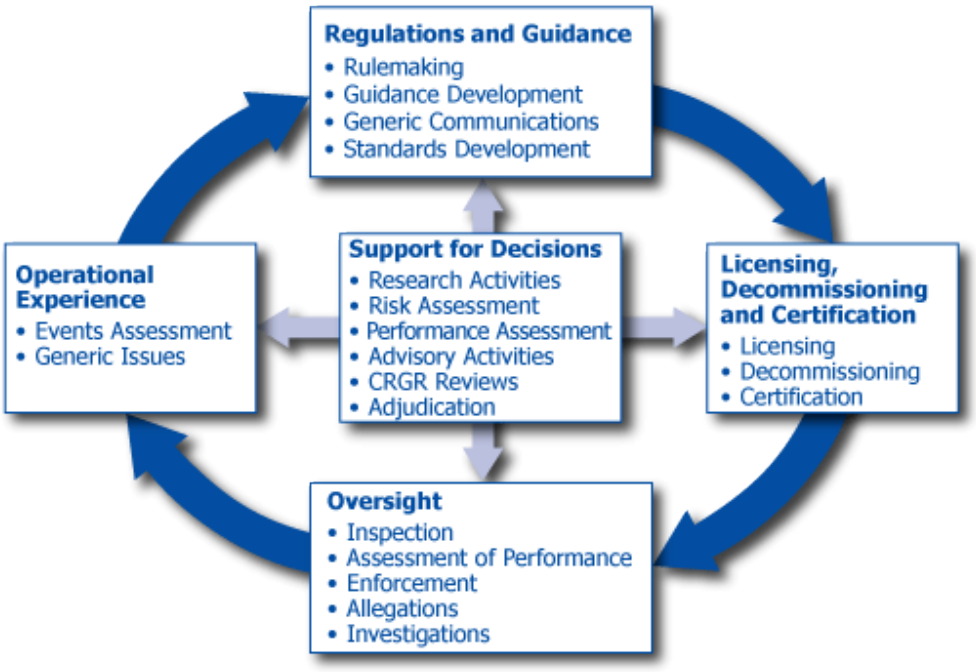


Figure 2: NRC Regulatory Program

Cybersecurity Activities

Much investment in time and resources has been made by the NRC to ensure that developers, operators, and maintainers of nuclear power facilities establish a cybersecurity program, and submit a plan to show compliance. The current key guideline they have put out to nuclear materials operators on cybersecurity is NRC RG 5.71, which currently in its Draft Final Rule. It spells out the requirements for a cybersecurity plan to be submitted by the licensees for the NRC's review and approval. The licensee is required to "provide high assurance that digital computer and communication systems and networks are adequately protected against cyber-attacks, up to and including the design basis threat as described in Title 10 of the Code of Federal regulations (10CFR) Part73, Section 73.1."

The provisions in RG 5.71 require protection of all critical systems and networks and require implementation of controls that will defend these systems against any cyber-attack that would adversely affect the availability, integrity and confidentiality of the critical system's assets and data. The protection of critical assets and data is to be achieved through the, "implementation of state-of-the-art defense-in-depth protective strategies" [RG 5.71 c (2)], whose aim "to ensure that the functions or tasks required to be performed by the critical assets … are maintained and carried out" [RG 5.71 c (4)] and "to prevent adverse effects from cyber-attacks" [RG5.71 c (3)]. The controls referred to in NIST 800.53 and the

recommendations relevant to those controls found in NIST 800.82, are defined in terms of three distinct classes: management, operational, and technical**.**

The NRC has disclosed that there are many items to address in ensuring better cybersecurity measures are in place that are compliant with the NRC's charter. Current efforts that it is investigating include:

- Involvement with several industry specific and international standards groups for setting cybersecurity standards. They believe the best way to develop standards is to work with outside resources to maximize resources and progress.
- Commitment to shared learning regarding cybersecurity through engaging other Federal agencies.
- Use of ISO 26262 "Road vehicles -- Functional safety" and it's reference standard, IEC 61508 Functional Safety standard for automotive Electric/Electronic Systems are important source documents for NRC.
- Continual reassessment of NRC RG 5.71 Cybersecurity Guide as the cybersecurity landscape changes and to fully understand risks.
- Standardization and improvement of architectures for nuclear management devices and equipment to include elements such as *Verification Tools and Diverse Redundancy "the power of 5" in testing for design flaws.*

NIST

NIST Special Publication 800 series of documents and the Federal Information Processing Standards Publication 199 *Standards for Security Categorization of Federal Information and Information Systems* (FIPS 199) are the baseline cybersecurity standards used by the Federal Government.

FIPS 199 is the mandatory standard to categorize all information and information systems collected or maintained by, or on behalf of, each Federal agency. FIPS 199 targets providing appropriate levels of information security according to impact of risks. This is the starting point for the use of the various NIST publications used to perform lifecycle security assessment, controls, and monitoring (as shown in Figure 3 below).

This process is again reminiscent of the lifecycle approach to Information Security discussed in Section 3.1 above. The added feature here is the various NIST standards publications that provide the guidance for each element of the security lifecycle are highlighted.

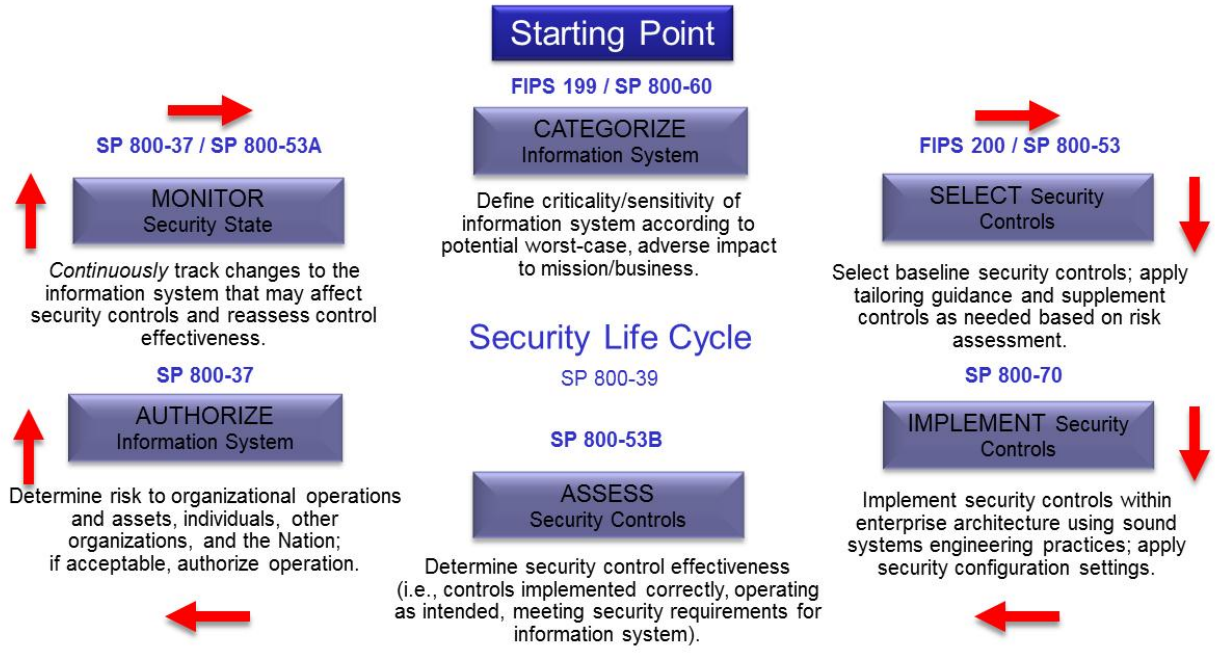


Figure 3: Security Lifecycle and Corresponding NIST Publications

NIST standards documents are valuable assets for the development of industry-specific cybersecurity guidance documents (e.g., NISTIR 7628 and others for Smart Grid).

2.3.4 Financial Payments

The financial payments industry has an interesting aspect that made it an appropriate industry to examine in this study— that of distributed risk. The financial payments industry has a complex ecosystem that includes banks, card associations (Visa, MasterCard, etc.), merchants, acquirers (generally seen as the bank or entity that the merchant uses to process their payment card transactions), etc. Each of these entities plays a part in handling payment transactions and the sensitive cardholder data associated with them, leading to an interesting "supply chain" issue with respect to data security. Figure 4 was originally intended to show an example of the payment processing and fees for a debit or credit transaction, but has been re-purposed here to show the interplay of various players in the payments ecosystem.

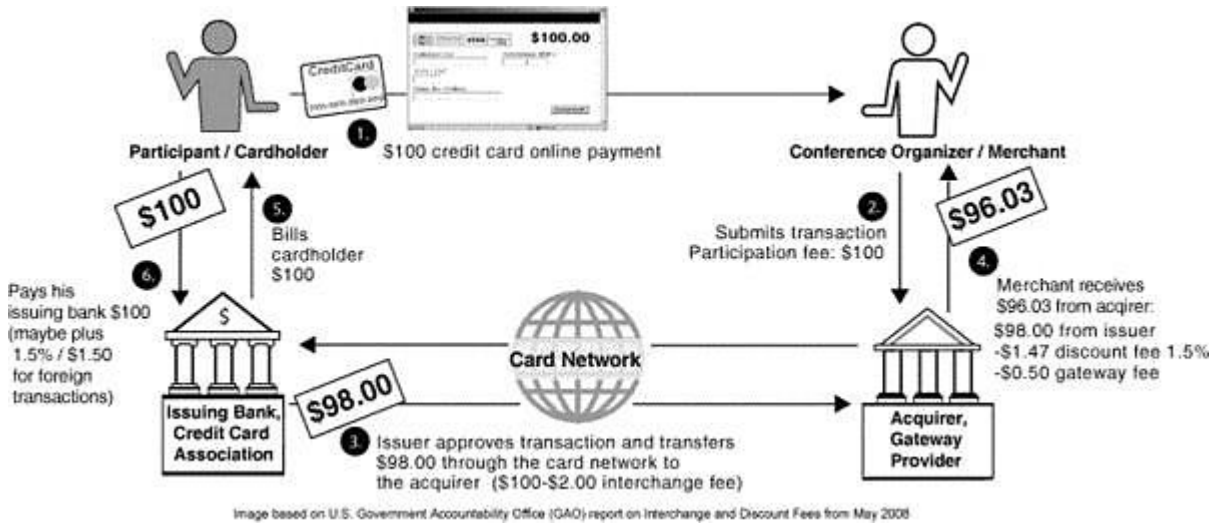


Figure 4: Financial Payment Ecosystem[ii]

This complex network of participants all of whom store or transmit cardholder sensitive information created a need to secure this distributed system. Many potential vulnerabilities surface that must be addressed and the financial payments industry, principally the card associations, or brands, led the development of payment card industry (PCI) standards for security of transaction and cardholder data. PCI standards mandate minimum-security requirements on all participating organizations in the distributed payment-processing ecosystem.

These PCI standards ensure the end-to-end security of the payment process for the entire supply chain. These fit with the security of the communications between the card and reader that entails securing the magnetic card swipe or the contactless card tap through encryption, key management, etc. This-card to-reader communications security was not germane to this research.

Regulation

Federal law is notably light on regulation of payment card data disclosure. The Dodd-Frank Wall Street Reform and Consumer Protection Act takes some steps toward security regulation in the establishment of a Consumer Protections Bureau with the Federal Reserve, but other attempts to create specific regulations and fines to control data security have made it through committee, but not to the floor for a vote.

These bills generally require that an entity handling or storing data above a certain volume be required to implement security protections, disclose breaches immediately, and provides a standard of fines. Thirty-eight States have data breach disclosure laws, with varying degrees of civil and criminal penalties for noncompliance. Tort liability among banks and merchants has been the standard method of enforcement and recently, Federal courts have set strong precedent for data breach tort liability in class-action suits as well. The total cost to merchants can range from $90 to $305 per breached *record*.

To take control of the costs of breaches, credit card brands now have a standard schedule of fines with much lower or zero costs for merchants that have been participating in the PCI compliance programs and disclose breaches immediately. They also maintain zero-liability programs for cardholders and standard agreements among banks in the network to expedite fraud defense and keep matters out of the courts. Essentially, the payment brand networks have responded to the public demand and implemented security policies that mirror Federal regulatory objectives. It should be noted however, that cost figures to implement PCI standards are not trivial. IT research company Gartner, Inc., reported in 2008 that among the Level 1 retailers surveyed, an average of $2.7 million was spent to become PCI compliant, excluding the costs of PCI assessment. This figure represented a five-fold increase from 2006 costs.[iii]

Payment Card Industry Data Security Standard

The vast majority of attention in the card payment systems security is focused on securing traditional servers that store sensitive data. The basic approach mirrors the security practices throughout the IT industry, with feedback from fraud management practice. The Payment Card Industry Security Standards Council (PCI-SSC) codifies these practices, a body comprised of the major credit card networks (see www.pcisecuritystandards.org/). It should be emphasized that the financial payments industry took a top-down approach in mandating the PCI-DSS. The PCI-SSC consists only of credit card network operators -- no merchants, acquirers, etc.

The standard mandates these practices and the enforcement model is distributed from the PCI-SSC to the individual network's security programs, to the acquirers, to the merchants, which are the targets of most of the standard's requirements. Although not directly involved with certification, the PCI-DSS provides certification requirements. These include yearly self-assessment for small merchants, and full audits by PCI-certified Qualified Security Assessors (QSAs) for large merchants, as well as quarterly network scans for all merchants. Payment applications have a similar program of standards and certification, the Payment Application Data Security Standard (PA-DSS). The actual standards are summarized in Table 3 below.

Table 3: PCI-DSS Objectives

Control Objectives	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software on all systems commonly affected by malware
	6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

These 12 basic principles of IT security are again reminiscent of the stages covered by the Information Security Lifecycle approach. They provide a best-practices defense and audit trail against known and unskilled attacks, which comprise the vast majority of the threats and have not changed significantly in recent years.

For the PCI-DSS certified systems that have experienced data loss, the majority were found to be improper certified, and the forensic evidence suggests that proper application of the PCI-DSS would have prevented the breach. Even with full adherence to the standard, however, there is still significant potential threat from specifically targeted zero-day and insider attacks because payment processing inherently requires the use and transmission of sensitive information throughout the processing chain of several parties.

Scanning and Assessment

PCI-DSS requires merchants to regularly scan their network environment and perform assessment to ensure compliance. Acquirers must collect this information from each merchant and report it to the security compliance program of the card networks, with differing requirements based on the merchant's annual transaction level. These transaction levels are not delineated by PCI, but are relatively standard among payment brands. Quarterly automated network scans with software from the PCI's list of approved scanning vendors. Annual in-depth assessments are also required, in the form of a self-assessment questionnaire (SAQ) or an on-site assessment by a PCI-SSC certified qualified security assessor, either internal or external.

Certification

For small merchants, depending on the payment brand requirements, the PCI-SSC provides a standard SAQ for PCI DSS compliance. Larger merchants and processors, however, are required by the payment brands to undergo regular scanning and assessment by council-certified vendors. The PCI-SSC maintains the programs for certification of approved scanning vendors, qualified security assessors for merchants, internal security assessors for issuers and acquirers, and payment application qualified security assessors for third-party processing applications.

The certification processes includes admission to the program, mandatory training, certification testing, ongoing compliance testing, and periodic recertification. To gain admission, a business must demonstrate legitimacy, independence, and insurance coverage, as well as to sign agreements and pay fees to the PCI-SSC. The business also must show that each of its assessors has at least one year of full-time experience in three specified security domains, a bachelor's degree, and a specified security industry certification. Additionally, the business must show that it has the facilities, equipment, capabilities, and procedures in place to handle the assessment work.

Training for assessor staff consists of an online course and test, followed by two-day live course. The PCI-SSC then oversees mock assessments, which may be ordered at their discretion, and recertifies staff. Yearly recertification requires compliance with the original requirements as well as continuing education credits assigned by the council. The PCI-SSC maintains lists of approved vendors and applications.

2.3.5 Medical Devices

The Food and Drug Administration emphasizes that cybersecurity for medical devices and their associated communication networks is a shared responsibility between medical device manufacturers and medical device user facilities. The proper maintenance of cybersecurity for medical devices and hospital networks is vitally important to public health because it ensures the integrity of the computer networks that support medical devices. Perhaps more importantly, those medical devices that monitor critical life functions and/or administer medicine have an elevated risk factor in terms of cyber-attack implications.

A rapidly growing cybersecurity problem can have devastating results to healthcare patients, and healthcare operations of all sizes. This escalating concern comes on the eve of rapid transition from conventional radiology-related capture methods to the growing digital picture archiving and communications systems (PACS).

Entire departments are being converted to digital imaging and reporting. Archived images are being scanned and stored on computer drives. In addition, diagnosis is being conducted from these same computer systems. It is entirely possible that a virus or worm can makes its way into such systems that can result in the destruction and hence the loss, or mishandled dispersion, of critical information.

Regulations in Place

FDA's Center for Devices and Radiological Health (CDRH) is responsible for regulating firms that manufacture, repackage, and/or import medical devices sold in the United States. In addition, CDRH regulates radiation-emitting electronic products (medical and non-medical) such as lasers, x-ray systems, ultrasound equipment, microwave ovens, and color televisions.

Medical devices are classified into Class 1, 2, and 3 with regulatory control increasing from Class 1 to Class 3. The device classification regulation defines the regulatory requirements for a general device type. Most Class 1 devices are exempt from Premarket Notification 510(k); most Class 2 devices require Premarket Notification 510(k); and most Class 3 devices require premarket approval.

Medical devices distributed in the United States are subject to General Controls─ pre-marketing and post marketing regulatory controls. The basic regulatory requirements that manufacturers of medical devices distributed in the United States must comply with are:

- Establishment Registration - 21 CFR Part 807;
- Medical Device Listing - 21CFR Part 807;
- Premarket Notification 510(k) - 21 CFR Part 807 Subpart E;
- Premarket Approval (PMA) - 21 CFR Part 814;
- Investigational Device Exemption (IDE) - 21CFR Part 812;
- Quality System Regulation (QS)/Good Manufacturing Practices (GMP) - 21 CFR Part 820;
- Labeling - 21 CFR Part 801; and
- Medical Device Reporting - 21 CFR Part 803.

Industry Issues

FDA is aware of misinterpretation of the regulations for the cybersecurity of medical devices that are connected to computer networks. Hospitals and device manufacturers do not agree on interpretation of roles and responsibilities in FDA regulations with respect to cybersecurity. To manage this process the FDA has issued a document on cybersecurity that strives to answer specific questions on the issue.

FDA's interpretation of the regulations can be found in the 2005 *Guidance for Industry - Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (January 14, 2005) and its accompanying information for healthcare organizations. FDA emphasizes the following:

- Medical device manufacturers and user facilities should work together to ensure that cybersecurity threats are addressed in a timely manner;
- The agency typically does not need to review or approve medical device software changes made for cybersecurity reasons;
- All software changes that address cybersecurity threats should be validated before installation to ensure they do not affect the safety and effectiveness of the medical devices;
- One of the more important questions is one of responsibility. The FDA makes it clear in 21 CFR 820.100 that the manufacturer is responsible stating that threats should be addressed directly to the manufacturer (The FDA also states in 21 CFR 820.30(i) that manufacturers need to validate any patches implemented (to ensure the device's safety and efficacy. However, device manufacturers have major concerns regarding validation of implementation of changes or patches to their software. Therefore, manufacturers typically do not take proactive action, or simply delay until delivery of software patches is necessary. Hospitals and care providers point out that the consequences of this inactivity can be devastating to the industry.

Enforcement Efforts

Most enforcement efforts are conducted with inspections and punitive damages for violations that hurt the medical device manufacture's profits and market position. When the FDA enforces its regulatory authority, it uses the following methods:

1. **Application Integrity Policy -** Regarding the integrity of data and information in applications submitted for FDA review and approval
2. **Bioresearch Monitoring Program (BIMO)** - On-site inspections and data audits designed to monitor all aspects of the conduct and reporting of FDA regulated research. The BIMO program was established to ensure the quality and integrity of data submitted to the agency in support of new product approvals, as well as, to provide for protection of the rights and welfare of the thousands of human subjects involved in FDA regulated research
3. **Disqualified/Restricted/Assurance List for Clinical Investigators-** Restricted from receiving investigational drugs, biologics, or devices if FDA determines that the investigator has repeatedly or deliberately failed to comply with regulatory requirements for studies or has submitted false information to the study's sponsor
4. **Electronic Records; Electronic Signatures, 21 CFR Part 11-** Background information and updates on the rule that allows the use of electronic records and electronic signatures for any record that is required to be kept and maintained by other FDA regulations
5. **FDA Debarment List -** Firms or individuals convicted of a felony under Federal law for conduct (by a firm) relating to the development or approval, including the process for development or approval, of any abbreviated drug application; or (an individual convicted) for conduct relating to development or approval of any drug product, or otherwise relating to any drug product under the Federal Food, Drug, and Cosmetic Act
6. **FDA Notice of Initiation of Disqualification Proceedings and Opportunity to Explain (NIDPOE) Letters -** A NIDPOE letter informs the recipient clinical investigator that FDA is initiating an administrative proceeding to determine whether the clinical investigator should be disqualified from receiving investigational products pursuant to the Food and Drug Administration's regulations. Generally, FDA issues a NIDPOE letter when it believes it has evidence that the clinical investigator repeatedly or deliberately violated FDA's regulations governing the proper conduct of clinical studies involving investigational products or submitted false information to the sponsor
7. **Public Health Service (PHS) Administrative Actions Listings-** Lists certain individuals who have had administrative actions imposed against them. The PHS Office of Research Integrity (ORI) maintains the list
8. **Reading Room (Electronic Freedom of Information Act) –** FDA's Office of Regulatory Affairs (ORA) documents frequently requested by the public through the Freedom of Information Act

New and Ongoing Challenges

Some of the challenges and issues FDA is focused on include the following.

Risk Assessment

- FDA has limited resources and is seeking good guidance in obtaining better cybersecurity controls for medical devices;) risk assessment is a huge challenge, and an evolving problem.
- Advances of ISO Standard 14971 (which is focused on RA) is a good engagement point to improve the FDA's risk mitigation position.

International Manufacturing

- There is an increasing set of problems due to medical devices and other FDA regulated items in general being manufactured overseas and importing sub-par devices.
- Punitive damages are harder to enforce and control in this international environment, and tighter controls are needed.
- FDA is currently performing more inspections to these international manufacturing sites to curtail and slow down mismanaged operations that try to circumvent FDA regulatory compliance via international law.

Engineering & Architectural Controls

- A new guidance document is needed to standardize and improve architectures for medical devices.
- FDA is working with NRC gain insight on how best to address component vendors.

2.3.6 Automotive

While not explicitly a subject for this study, the automotive industry began to come into focus in the latter stages of the research process. A next step was an examination of how best practices from other industries could affect the need for cybersecurity in the automotive industry. Some key activities helped this shift into examining the needs of the automotive industry, which are described below.

European Activities

Several European programs have produced helpful information on this subject. First, the E-Safety Vehicle Intrusion Protected Applications (EVITA) program is a 3-year, $6 million project that completed in December 2011; a prototype demonstration occurred at the November ESCAR conference.

Second is the ESCAR conference now in its ninth year. The proceedings of each annual conference are published and available free of charge on the ESCAR conference Web site at www.escar.info/index.php?id=12.

Third, the Infineon SME interview yielded discussion of the development of new CAN bus alternatives that are based on time-triggered protocol. Examples include the FlexRay approach being fielded in high-end German models. FlexRay was developed by the FlexRay consortium, whose membership included multiple automotive OEMs, suppliers, and microcontroller technology vendors such as Motorola, Philips, and ST Micro.

The SAE Security Committee actively discusses leading edge approaches to automotive security. This discussion has included the European research efforts.

SAE Security Committee

NHTSA is a non-voting liaison member participating in the SAE Security Committee (Web site at www.sae.org/servlets/works/committeeHome.do?comtID=TEVEES18). Members of the committee tend to be functional safety engineers and system/hardware/software developers.

The cybersecurity skillset does not often reside in operational competency areas - even if the labor resources are technical in nature. The cybersecurity skillset historically is deemed a function of IT personnel—the CIO, chief security officer (CSO), and subordinates. The designers and operators of operational systems should acquire these skillsets. We observed this in all industries studied.

The SAE Security Committee's mission is to develop and maintain recommended practices and information reports in the area of vehicle electrical systems' security. The committee's scope is on-board vehicle electrical systems that affect vehicle control or otherwise act contrary to the occupants' interests if the systems are manipulated by an attacker.

The goals of the committee are:

- To identify and recommend strategies and techniques related to preventing and detecting adversarial breaches, and
- Mitigating undesirable effects if a breach is achieved.

The SAE Security Committee submitted a response to the Request for Information (RFI). Their response is discussed in the RFI section below. The group seems to be involved in general cybersecurity best practices information gathering having investigated both the EVITA program and the NIST cybersecurity standards documents. They are focused on not only building their cybersecurity body of knowledge, but also finding a baseline document to use to develop automotive industry-specific cybersecurity guidelines.

EVITA

The objective of EVITA is to design, verify, and prototype a modular, cost-efficient security solution for automotive on-board networks. This will protect sensitive data within such networks against compromise and, in doing so, enable secure communication among cars and between cars and infrastructure.

Some high-level background on EVITA:

- Consortium of European private sector, OEM (BMW), and suppliers as well as academia
- Effort funded by the European Commission and consumed 3 years and $6 million (50% matched by consortium members).
- The EVITA Security Risk Management approach drew upon cybersecurity risk management best practices in cybersecurity (NIST standards) and functional safety (ISO 26262).
- The EVITA Security Risk Management approach is a candidate for use as a baseline for a tailored Risk Management Guideline for the SAE Security Committee.

It is to be determined if the technical Hardware Security Module (HSM) specification is an appropriate source for a baseline technical security specification in the United States. However, as noted above, EVITA's proposed Security Risk Management approach may be beneficial as baseline guidance for the U.S. automotive industry. Using these security guidelines as a baseline in the U.S. automotive industry

will leverage the EVITA work that modified cybersecurity and functional safety best practices to delineate automotive industry-specific guidelines.

2.4 Request for Information

The RFI for *Cybersecurity and Safety of Motor Vehicles Equipped with Electronic Control Systems* was released on August 2, 2011. Of the 13 responses that were received, three in particular are noteworthy.

SAE Security Committee

First, the SAE Security Committee submitted a response. The highlights of this response included the identification of the EVITA project as having done "significant work in the area of automotive security risk assessment" and added "the committee feels that this [EVITA] is a subject that will need additional investigation as the industry continues to work in the area cybersecurity."

Another noteworthy issue in the response is that "currently the CAN protocol has no explicit support for security mechanisms," and "…it is challenging to add effective security layered on top of the protocol", finally, adding that "the committee will likely also investigate techniques to secure other in-vehicle networking technologies."

The last significant suggestion of the SAE Security Committee is that an Information Sharing and Analysis Center (ISAC) would be beneficial. However, the committee noted that, due to the participation of competitive private sector suppliers and OEMs within SAE, and owing to the need to openly share sensitive information about risks and vulnerabilities, SAE would not be the appropriate forum for an ISAC.

EVITA

EVITA focused much of its response on the technology solution the EVITA project developed - the Hardware Security Module (HSM).

By virtue of both their RFI response and ongoing conversations, it is believed that the automotive industry-specific cybersecurity guidelines developed by EVITA could be a basis for the US industry. Beyond the discussion of the HSM approach, the EVITA submission yielded two intriguing points:

1. Delineating potential attacks and related security requirements served as the starting point for developing a technical solution
2. V2X security efforts are focused on the V2X communication and vehicles and infrastructure in the connected vehicle ecosystem must be secure.

This second point is especially important. The EVITA consortium is stating that in a V2X world, security should be examined holistically from end-to-end. The vehicle itself─ the in-vehicle network and its security from "the outside world," as well as the security of any roadside infrastructure, should be addressed in addition *to* the security of the communications and V2X transactions. This is a key observation for the U.S. marketplace with respect to connected vehicle development.

Toyota

The Toyota response yielded two issues worth noting:

1. It highlighted the importance of determining accountability for security countermeasures'
2. It highlighted the necessity for developing cybersecurity countermeasures within the on-board diagnostics (OBD) protocol.

2.5 Challenges and Issues

This section brings together the various challenges and issues seen throughout the industries studied. When formulating a strategy regarding cybersecurity in the automotive industry the following challenges and issues are important:

- The transportation mission is currently safety focused not security focused.
  - Transportation modes are now correlating security and safety; one can't have a safe system without it being a secure system

- There is a perception that there is "no Return on Investment for security."
  - But what is the "cost" of a security breach (monetary, liability, loss of good name, etc.)? It depends on the severity of the outcome.

- Operations systems now use Information Technology and wireless communications extensively.
  - Systems are no longer closed; they are connected through IT and Communications and are inherently more vulnerable and hackers now know about them.
  - IT security best practices are being applied to operational systems.

- The normal approach to cybersecurity of operational systems, hardware, and software is to add security measures after they are developed and fielded.

- Skillsets for cybersecurity tend to lie in the IT core competency and are not resident in the developers of operations systems, hardware, and software.

2.6 Observations

The research of the various industries studied has yielded some best practices for consideration. These best practices may become elements of a strategic cybersecurity roadmap. Attributions to industries where the finding was derived are in parentheses.

Cybersecurity is a lifecycle process that includes elements of assessment, design, implementation, and operations as well as an effective testing and certification program. (All Industries)

Multiple industries studied all point to the need to be continually vigilant in securing systems, networks, hardware, and software.

The aviation industry has some similarities to the automotive industry (FAA)

The aviation industry and automotive industry share some similarities. Vehicles and aircraft are both becoming extensively eEnabled and connected. Additionally, the migration to the NEXTGEN air traffic control environment mirrors the development of the Cooperative Vehicle environment, both yielding exponentially more issues with respect to cybersecurity vulnerabilities. NHTSA and FAA have very different statutory authorities.

Leadership from the Federal government can help the development of industry-specific cybersecurity standards, guidelines, and best practices (FAA)

It was observed that leadership from the Federal government can help the development of industry-specific cybersecurity standards, guidelines, and best practices. Some industries support the idea of Federal minimum-security requirements.

Ongoing shared learning with other Federal Government agencies is beneficial (FAA, NRC, FDA, NIST)

This research was a first step in the process of elevating NHTSA's baseline knowledge of cybersecurity. The learning process should continue through ongoing cooperation with key government agencies such as FAA, NRC, FDA, and NIST. In particular, FAA is moving toward rulemaking. FAA has done much learning in concert with the NRC as an example and FAA subject matter experts referenced NRC activities on several occasions.

Use of NIST Cybersecurity Standards is a way to accelerate development of an industry-specific cybersecurity guideline (All Industries)

The NIST cybersecurity suite of standards documents is often used as a baseline to industry-specific security guidelines.

International cybersecurity efforts are an important source of information (FAA, automotive)

The research has revealed several efforts in Europe that have been ongoing and show some success addressing cybersecurity issues. Examples are:

- The annual ESCAR Conference, which highlights security developments, is in its 9th year.

- The FlexRay Consortium developed an alternative approach to the CAN communications bus based on Time-Triggered Protocol that addresses a baseline security issue in the CAN approach.
- The EVITA security guidelines documents.

Consider developing a cybersecurity simulator that can facilitate identification of vulnerabilities and risk mitigation strategies (FAA)

FAA engaged the Volpe Center to work with academia to develop the ANSS and initially do "white hat" hacking exercises to highlight vulnerabilities in the Gatelink, a vital device that communications flight data with aircraft at the gate.

While this laboratory environment has been valuable for collaborative learning between government, academia, private sector, and internationally, FAA is now beginning rulemaking (discussed above) and will use the ANSS to examine each of their identified eEnabled "points of pain" as a starting point to the rulemaking process.

There should be cybersecurity standards for the entire supply chain (financial payments, automotive)

This was a key observation from the financial payments industry, which has a unique distributed risk model since the financial payments network is a complicated ecosystem where many organizations handle sensitive transaction and cardholder data. The card associations (Visa, MasterCard, etc.) formed the Payment Card Industry Security Standards Council (PCI-SSC) and developed the Payment Card Industry Data Security Standard (PCI-DSS). All those in the payment-processing ecosystem mandate PCI-DSS for use. This requirement can be a model for the need to ensure security throughout the supply chain (both pre-production and post-sale) in the automotive industry.

Foster industry cybersecurity groups

Establishing an Information Sharing and Analysis Center (ISAC) and an automotive industry Cybersecurity Emergency Response Team (CERT) should be investigated. CERTs act as a resource for cybersecurity professionals to highlight cybersecurity incidents and provide support for incident response and forensic analysis as well as act as a conduit for topical cybersecurity information. For example, Federal agencies are required identify IT breaches to US-CERT. US-CERT then follows their procedures for examination and mitigation of the breach.

ISACs are extremely valuable, cross-industry organizations that act as clearinghouses for information on cyber and physical threats, vulnerabilities, and solutions. They help members better understand their threats and vulnerabilities and are forums for anonymous submission regarding specific vulnerabilities and security breaches. The SAE Security Committee highlighted the need for an automotive industry ISAC in their RFI response.

Use Professional Capacity Building to develop cybersecurity skillsets in system designers and engineers (All)

Many industries see a disconnect between the security skillsets of the technical resources developing operation systems and those needed. Traditionally cybersecurity has been seen as the domain of the IT department, but this is clearly no longer the case. Momentum is gaining in the US automotive industry due to the Toyota Camry sudden acceleration incident in 2010 and the various academic research projects demonstrating the vulnerabilities of modern vehicles.

Connected Vehicle security should be end-to-end; vehicles, infrastructure, and V2X communication should all be secure (aviation, automotive [specifically EVITA])

This was an issue highlighted by EVITA in their RFI submission. They stated that in their research of various European V2X security efforts, none were examining security beyond the communications itself. Rather, these security efforts simply noted that vehicles and infrastructure must be secure. Therefore, there is a strong need for NHTSA and the Intelligent Transportation Systems Joint Program Office to work together to ensure end-to-end security in a Connected Vehicle world.

Mapping Best Practices to the Information Security Lifecycle

Mapping these key observations to the process of a lifecycle information security program is a good exercise to show a process that may provide input to NHTSA's development of a strategic roadmap. First, Figure 5 provides a reminder of what the Information Security Lifecycle Process entails.

Figure 5: Information Security Lifecycle Process

The key observations are mapped to this lifecycle process in Figure 6.

Best Practice Examples Identified	Establishing a Security Policy	System Security Evaluation	Iterative Risk Assessment	System Prioritization	Security Architecture	Remediation and Implementation	Security Test and Evaluation	Awareness and Security Training	Intrusion Detection and Response
	Assess					Design		Implement	Operate
Aviation As Parallel Industry	✓	✓	✓	✓	✓	✓	✓	✓	✓
Strong Federal Leadership	✓	✓	✓	✓	✓	✓	✓	✓	✓
End-to-End Connected Vehicle Security	✓	✓	✓	✓	✓	✓	✓	✓	✓
Leveraging International Cybersecurity Efforts	✓			✓	✓			✓	
Fostering Industry Cybersecurity Groups	✓				✓	✓		✓	✓
Ongoing Shared Learnings With Other Federal Agencies	✓	✓			✓	✓		✓	✓
Cybersecurity Is A Lifecycle Process	✓	✓	✓	✓	✓	✓	✓	✓	✓
Cybersecurity Standards For Entire Supply Chain	✓				✓	✓	✓		
System Design And Operators Cyber Acumen	✓	✓	✓	✓	✓	✓	✓	✓	
Identify Minimum Security Requirements	✓	✓	✓	✓	✓	✓	✓	✓	✓
Develop A Cybersecurity Simulator		✓	✓	✓	✓	✓	✓	✓	✓
Identify A Standards Development Baseline	✓	✓	✓	✓	✓	✓	✓	✓	

Figure 6: Key Observations Mapped to the Lifecycle Process

2.7 References

[i] U.S. Department of Transportation. (2011, August). Cyber security and safety of motor vehicles equipped with electronic control systems (RFI Solicitation Number: DTRT57-11-SS-00007). Retrieved from www.fbo.gov/spg/DOT/RITA/VNTSC/DTRT57-11-SS-00007/listing.html

[ii] Government Accountability Office. (2009, November 19). Credit cards rising interchange fees have increased costs for merchants, but options for reducing fees pose challenges. (Report No. GAO-10-4). Washington, DC: Author.

[iii] Cost of PCI Compliance. (2009, September 17). (Web oage). PCI DSS Compliance Blog. Retrieved from http://blog.elementps.com/element_payment_solutions/2009/02/pci-compliance-costs.html

DOT HS 812 075
October 2014

U.S. Department
of Transportation
**National Highway
Traffic Safety
Administration**

10929-100814-v3