Developing a Framework to Improve Critical Infrastructure Cybersecurity

Response to Request for Information Number: 78 FR 13024
Issued February 26, 2013

Prepared for
Department of Commerce
National Institute of Standards and Technology

Date: April 8, 2013

Submitted By:

Electrosoft Services, Inc.
1893 Metro Center Drive (formerly 11417 Sunset Hills Road), Suite 228
Reston, VA 20190
Tel: (703) 437-9451 Fax: (703) 437-9452
http://www.electrosoft-inc.com

Electrosoft
Managing Cyber Security Risk through Innovation and Engineering

Contents

1 Introduction

This section describes our understanding of the requirements and introduces Electrosoft as a credible contributor for providing inputs to the National Institute of Standards and Technology (NIST) for Developing a Framework to Improve Critical Infrastructure Cybersecurity.

1.1 Our Understanding of the Requirement

The National Institute of Standards and Technology (NIST) is conducting a comprehensive review to develop a framework to reduce cyber risks to critical infrastructure. The Framework will consist of standards, methodologies, procedures and processes that align policy, business and technological approaches to address cyber risks.

NIST is requesting information from industry to help identify, refine and guide the many interrelated considerations, challenges and efforts needed to develop the Framework. In developing the Cybersecurity Framework, NIST will consult with the Secretary of Homeland Security, the National Security Agency, Sector-Specific Agencies and other interested agencies including the Office of Management and Budget, owners and operators of critical infrastructure and other stakeholders including other relevant agencies, independent regulatory agencies, State, local, territorial and tribal governments. The Framework will be developed through an open public review and comment process that will include workshops and other opportunities to provide input.

1.2 Introducing Electrosoft

Electrosoft Services, Inc. (Electrosoft) is an Information Technology (IT) professional services company that delivers cybersecurity services and solutions to enable our customers to manage risk, achieve compliance and secure their systems. We have been serving the Federal Government since 2001, assisting various departments and agencies including the Department of Veterans Affairs (VA), National Institute of Standards and Technology (NIST), the Department of Treasury, General Services Administration (GSA), Department of Commerce (DOC), Department of Health and Human Services (HHS), Department of Defense (DOD), Federal Aviation Administration (FAA), Department of Homeland Security (DHS), US Patent and Trademark Office (USPTO), Environmental Protection Agency (EPA) and others. Our offices are located in the National Capital Region, 25 miles from Washington, DC, in Reston, Virginia.

Electrosoft Socio-Economic Certifications
Small Disadvantaged Business (SDB) certified by the US Small Business Administration
Economically Disadvantaged Woman-Owned Small Business (EDWOSB) per US Small Business Administration
Small, Woman-Owned and Minority-Owned Business (SWaM) certified by State of Virginia

Socio-economic Status and Self Certification. Electrosoft is a Small Disadvantaged Business (SDB), an Economically Disadvantaged Woman-Owned Small Business (EDWOSB), and a Small, Woman-Owned and Minority-Owned (SWaM) Business certified by the State of Virginia.

Cleared Facility and Staff. We have a TOP SECRET facility clearance granted by the Defense Security Service (DSS), and personnel with SECRET and TOP SECRET clearances.

ISO 9001:2008 Quality Management System. We take great pride in the quality and consistency of our services, and have established documented quality processes to ensure that we consistently meet the requirements of each of our contracts and tasks. We have solidified our commitment to quality in certifying our quality management system to be ISO 9001:2008 registered (Certificate Number is TRC 00545).

Awards. Electrosoft's many awards include multiple certificates of appreciation from GSA, HHS, and NIST for outstanding service; being named to Inc. 500|5000 List for 2009, 2010 and 2011; Washington Technology's Fast Fifty for 2006; top 100 business in Virginia in the categories of diversity-owned, minority-owned, and woman-owned; 25 powerful minority women in business; outstanding 50 Asian Americans in business and 50 influential minorities in business.

1.3 Our Credibility for Effectively Contributing to this Effort

We believe that we offer strong credibility in contributing to this NIST effort to obtain feedback from industry stakeholders. The subsections below substantiate our knowledge and experience relevant to this effort.

1.3.1 Established NIST Partner

Electrosoft has been a trusted partner for the NIST Computer Security Division (CSD) since 2001. In this role, we have developed standards, guidelines, test frameworks, demonstrations, reference implementations and software tools for Identity Management, Personal Identity Verification (PIV), FISMA and Smart Grid. We understand NIST's unique mission within the Federal Government to promote innovation and industrial competitiveness by advancing measurement science, standards and technology. In supporting the NIST CSD, we have helped to drive research and development of test methods and standards for information technology to improve the usability, reliability and security of computers and computer networks.

Over the past ten years, Electrosoft has established a track record of meeting and exceeding expectations and requirements on NIST contracts. We have provided valuable recommendations to improve the quality and effectiveness of NIST program, such as our thought leadership in many areas of the FIPS 201 standard. We offered innovative ideas and recommendations for new guidelines for Federal IT security operations, such as NIST SP 800-79-1, *Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations* and NIST SP 800-128, *Guidelines for Security Configuration Management of Federal Information Systems*.

As shown by our many years of successful engagements with NIST, Team Electrosoft offers exceptional subject matter expertise, high-quality, proven dependability, excellent teamwork/collaboration and a deep understanding of the NIST mission.

1.3.2 Depth of Relevant Technical Experience

Our team includes world class experts in cybersecurity who have worked with the NIST CSD for over a decade to define and develop standards and guidelines for cybersecurity. We are actively engaged in efforts that influence policies and legislation in areas related to identity management (NSTIC National Program Office support), health information technology (VHA Security Analyst Services) and implemented programs (GSA FIPS 201 Evaluation Program) that support OMB policies related to HSPD-12.

We are currently assisting NIST in launching the NCCoE and are very familiar with its overall goals, objectives and operational model. Electrosoft has full depth and breadth of experience in all of the areas and dimensions of relevance to this requirement including policy, cybersecurity and metrics.

Other areas of relevant expertise include:

- Electrosoft supports the VHA Health Information Governance organization in identifying, analyzing and responding to policies and legislation related to cybersecurity and health IT. Our work supports the VHA Security Architect in developing and refining security architectures, models and business architectures for the VHA's next generation systems and services.
- Electrosoft supports the NIST Program Office for National Strategy for Trusted Identities in Cyberspace (NSTIC) - our efforts help to drive governance and policies in the area of identity and access management.
- Electrosoft conducted an extensive security architecture planning activity for the HHS OCIO in which we analyzed the security architecture plans (or comparable documents) for the HHS Operational Divisions through document reviews, interviews and other data collection methods

1.3.3 Smart Grid

Electrosoft has experience with NIST's work in the area of Smart Grid interoperability and security. We performed a survey of standards conformance methods in the electric sector and developed NISTIR 7823 (Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework) and also developed a White Paper on Automating Smart Grid Security.

2 Question Responses

Electrosoft provides cyber security consulting services, primarily to the Federal Government. While we do not have direct experience operating critical infrastructure systems, we have worked with numerous stakeholders through our support of the Smart Grid Interoperability Panel (SGIP) and during the development of NISTIR 7823 (Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework). We also performed a thorough survey of security standards and conformance methods used in the energy sector, which provided insight into SCADA and other ICS technologies. We are familiar with ISA-99 and NERC CIP as well as guidance from NIST on ICS and Smart Grid, but we will leave comments on implementation of those methods to the organizations more directly affected.

We have provided responses below to the questions pertaining to our areas of expertise.

2.1 Ideas for the Framework

We believe that the Cyber Framework will include standards and technology implementation guidance in common areas of cybersecurity such as the domains presented in the Energy Subsector Cybersecurity Capabilities Maturity Model:

- Risk Management
- Asset, Change and Configuration Management
- Identity and Access Management
- Threat and Vulnerability Management
- Situational Awareness
- Information Sharing and Communications
- Event and Incident Response
- Supply Chain and Dependencies
- Workforce Management
- Program Management

We believe that many of the approaches that have been developed for security in the IT sector are applicable to Critical Infrastructure cyber security. Several of the domains listed above are covered by various aspects of the Security Content Automation Protocol (SCAP) and we believe that the Cyber Framework should promote security automation techniques such as SCAP. As discussed in our White Paper on Automating Smart Grid Security, which was submitted to NIST CSD in 2011, the technology can be used in the following ways to improve Smart Grid and Industrial Control System security:

- Adopt the Asset Identification Format for Smart Grid Component Inventories
- Enhance ICS-CERT Security Advisories with Vulnerability Scoring
- Use of Asset Reporting Format for Interoperable Compliance Reporting
- Utilize Common Platform Enumeration
- Utilize Common Vulnerability Enumeration
- Develop OVAL-like checking engines for ICS Systems
- Automate Continuous Monitoring
- Develop Security Checklists for Systems

We will speak to what we believe are the overall goals of the Cyber Framework. Implementers of the framework will have to determine whether getting industry to reach those goals will involve voluntary compliance, positive / negative incentives or mandatory compliance.

2.2 Response to Questions for Current Risk Management Processes

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

There is currently no clear roadmap for critical infrastructure organizations to follow in order to achieve their cybersecurity practices. NIST's Cyber Framework provides an excellent opportunity to rectify the problem, and may provide incentives for the organizational and technological changes that will be needed to achieve higher assurance in the integrity and safety of these critical systems.

ICS systems have been developed to solve engineering problems but cybersecurity has not been a focus of their design. Traditional SCADA protocols such as ModBus and DMP3 (prior to version 5) do not include authentication, for example. Systems were built on these insecure protocols because they were designed with physical network isolation to achieve security. As these systems are connected to the internet, assumptions about physical isolation can result in serious security holes. These holes should be identified and tracked as known vulnerabilities so that their threat to real-world systems can be determined by the owners of affected assets and remedial actions may be taken. For several years, the Industrial Control System Cyber Emergency Response Team (ICS-CERT) has published security advisories and vulnerability announcements, as well as increasing numbers of ICS products are showing up in the National Vulnerability Database; these are both good signs.

To make use of these information resources, owners of critical infrastructure systems should develop asset inventories to enable accurate vulnerability scoring. A well-developed asset inventory will include information about hardware, OS and applications including versions and configurations, expressed in a standardized format. Use of a common naming convention for the components of the system enables all parties to understand what systems are being referred to and will enable automated vulnerability scoring. The Security Content Automation Protocol (SCAP) includes a standard for Asset Identification and a Common Platform Enumeration; we believe that these should be used by industry as they develop their asset inventories for risk management purposes.

Even after addressing problems such as a lack of challenge/response protocols for authentication, identity management remains a key area for improvement in many systems. As many ICS systems rely on default credentials for SCADA control, role-based authentication is frequently used and contractor access to controls systems is widely utilized but not closely managed. Devices are deployed in the field with default passwords, with the result that compromising one device enables access to the entire system. A password-based system provides little to no security when passwords are obtainable from user manuals or shared among numerous organizations and seldom changed. The purpose of authenticating users of control systems is to provide accountability for the activities that take place. For example, it should be possible for SCADA control messages to be traced to authorized individuals or systems. In such a system environment, individuals can be then held accountable for activities within the system.

Use Case: DNP3

SCADA systems frequently run on DNP3, which is frequently cited as being an unauthenticated

protocol. DNP3 version 5 is under development and an important new feature is Secure Authentication, specified in IEC 62341-5. Secure Authentication is an optional feature which enables symmetric and asymmetric cryptographic functions for authenticating communicating parties. Vendors are implementing Secure Authentication and utilities are being encouraged to deploy it. However, correct implementation requires more than purchasing the equipment that supports the correct version of the protocol. With the addition of cryptographic techniques come key management considerations that will require policy and procedures to implement in a secure manner. The industry overall would benefit from the development of publicly available checklists and rules for correct implementation of DNP3 Secure Authentication systems, as a missed implementation item can mean an insecure implementation.

The Cyber Framework may include the development of technology specific product and deployment checklists that can be used to determine how the deployed system will conform to the profile. For DNP3 systems, the checklist could include questions such as:

- Which DNP3 options are available?
- Are pre-shared keys used? If so, how are they generated and distributed to devices? How are they managed subsequently?
- Are asymmetric keys used? How are keys provisioned to devices in a secure manner? How is trust managed in the system?
- Are keys updated according to the recommended schedule in the standard? What is the update process?

The answers to these questions will enable rating a system's security against various threats. For example, if pre-shared keys are generated in the factory and shared in devices sold to multiple utilities, no one customer will be able to control or detect whether those keys are compromised. Even when keys are generated by the customer, they should be updated on the recommended schedule.

A system checklist will request inventories of the specific hardware, operating system and applications that make up the system, the policies that the system adheres to and the procedures put in place to implement those policies, and the system configuration settings that are selected to enable those policies.

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

The Department of Homeland Security Office of Inspector General report OIG-13-39 emphasizes that information sharing between critical infrastructure stakeholders is necessary to improve cybersecurity practices and we agree with that conclusion. The document identifies 18 industry sectors within critical infrastructure and observes that these sectors are experiencing threats including large scale denial of service attacks, network infiltration and attacks including spear phishing and social engineering of their help desks. The report calls on DHS to promote collaboration with sector-specific agencies with the aim of effective sharing of cybersecurity information. While technology and organizations will vary greatly across different sectors, many of the fundamental cybersecurity issues remain the same. Each sector will have domain-specific information about how systems are deployed and managed, which will be necessary input in determining how these systems should be protected.

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

Like many service providers with corporate offices, Electrosoft requires telecommunications, energy, financial services and water in order to conduct business.

2.3 Response to Question for Use of Frameworks, Standards, Guidelines, and Best Practices

1. **What additional approaches already exist?**

We believe NIST's guidance for IT cybersecurity (such as the FISMA guidelines and the Security Content Automation Protocol (SCAP) protocol) is applicable to critical infrastructure and ICS systems and should form the basis for the Cyber Framework. While specific security controls may not be implemented the same for ICS, management of security and system security assessment practices are equally applicable in many sectors and a common approach will support an interoperable system as cross-sector communications and dependencies continue to develop.

The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) published 31, May 2012, is a very good instrument for identifying generally where organizations stand in their cybersecurity practices, and "as written" is certainly applicable to more sectors than just electricity. The document defines the ten model domains of risk management, asset, change and configuration management, identity and access management, threat and vulnerability management, situational awareness, information sharing and communications, event and incident response and continuity of operations, supply chain and dependencies, workforce management and cybersecurity program management. For each model domain, it defines a number of Maturity Indicator Levels (MIL) for which MIL1 represents an initial but possibly ad-hoc capability. MIL2 represents the capability being performed by the organization, including documented practices, identified and involved stakeholders, adequacy of resources and standard processes to guide implementation. MIL3 is further institutionalization of the practices, including activities guided by policy and governance, conformance reviews, clear responsibilities and adequacy of resource skills and training.

We also believe that the document would benefit from the definition of an additional MIL4 in which the institutional cybersecurity practices are complemented by automated security such as the capabilities provided by SCAP. Utilizing common formats for asset identification, a common reporting format and benchmarks would all be useful tools in enabling information sharing and security planning among multiple stakeholders.

2. **Which of these approaches apply across sectors?**

The capability model described in ES-C2M2 could be readily applied to other sectors.