Chemical Sector Guidance for Implementing the NIST Cybersecurity Framework and the ACC Responsible Care® Security Code

ACC Chemical Information Technology Council (ChemITC)

January 2016

Legal and Copyright Notice

IMPORTANT: *This document is presented by the American Chemistry Council's (ACC) Chemical Information Technology Council (ChemITC) in an effort to provide some helpful ideas and guidance to assist persons already sophisticated and experienced in cyber security practices for the chemical industry.*

Information contained in the document is necessarily general in nature and is not to be considered a standard or directive that readers are obligated to follow. Instead, readers must independently determine what constitutes appropriate cyber security practice relative to their own needs and circumstances. Readers may need to adopt practices different from those discussed in this document, or employ practices that are not discussed herein, based on their factual situations, the practicality and effectiveness of particular actions and economic and technological feasibility. In making this determination, readers should consider information such as references noted in the document as well as other information that may be relevant. Readers should consult with legal counsel to ascertain their actions comply with relevant federal, state, and local law.

Although the information provided in this document is offered in good faith, and believed accurate based upon information available to preparers of the document, neither ACC, ChemITC, nor their individual member companies or employees, makes any warranty or representation, either express or implied, with respect to the accuracy or completeness of the information contained herein; nor do these organizations and individuals assume any liability or responsibility for reliance on any product, process or other information disclosed herein, or represent that its use would not infringe privately owned rights. None of the aforementioned parties shall be liable for any loss, damage or claim with respect to this document. All liabilities, including direct, special, indirect or consequential damages, are expressly disclaimed.

New information may be developed subsequent to publication that affects the document's completeness or accuracy. ACC and ChemITC assume no responsibility to revise the document to reflect any information that becomes available after its publication. Notwithstanding, because this document could possibly be revised periodically, the reader is advised to visit the ChemITC Web site or the MemberExchange site to obtain the most current version.

Introduction

This document provides members with practical guidance on the application of the NIST Cybersecurity Framework[1] as part of demonstrating compliance to the Responsible Care® Security Code[2] of Management Practices, specifically section 4 (Information and Cybersecurity). The Management Practices are currently being updated and will be available shortly from ACC.[3] The reader should be familiar with the major elements of both the *NIST Cyber Framework* and the ACC Responsible Care Security Code prior to applying the concepts in this document.

This guidance is based on the collective experience of members of the sector. The acceptance and use of this guidance should always be relative to the risk. It may be appropriate to go beyond the NIST Cyber Framework and this guidance based on your specific company requirements. Member notes (represented in Column K) on implementing the NIST guidance are available on the ACC ChemITC – IT Security Information Sharing Technology Workgroup area of MemberExchange[4]. The reader should also be familiar with the "Chemical Sector Framework Implementation Guidance" prepared by the U.S. Department of Homeland Security.[5]

This guidance is intended to be an "evergreen" document. All comments and suggestions for revisions should be directed to: info@chemitc.com.

Method

The method used to develop the guidance in this document begins with a review of the Responsible Care® Security Code and the NIST Framework document, with particular emphasis on the structure of the Framework core that is contained in appendix A. This core includes five distinct functions (Identify, Protect, Detect, Respond and Recover), each of which is further decomposed into several categories.

Each of these categories is reviewed considering several basic questions:

1) Is there more clarity to offer?
2) Is there something special about the chemical sector (compared to other manufacturing industries)?
3) Is there something of high importance to emphasize?

The result of this analysis is a list of recommendations and considerations (guidance) for each of the above five functions. This guidance is specific to the chemical sector, and aligns to the Responsible Care® Security Code.

Responsible Care Security Code

Cyber-related elements of the ACC Responsible Care Security Code include:

"Companies will apply the security practices identified in this Code to their cyber assets as well as their physical assets. Information networks and systems are as critical to a company's success as its manufacturing and distribution systems. Special consideration should be given to systems that support e-commerce, business management, telecommunications and process controls. Actions can

[1] http://www.nist.gov/cyberframework/
[2] http://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Responsible-Care-Security-Code
[3] "Responsible Care Security Code Implementation Guide: Site/Value Chain/Cyber", 2016
[4] https://memberexchange.americanchemistry.com/ISTWG/
[5] "Chemical Sector Cybersecurity Framework Implementation Guidance", 2016.

include additional intrusion detection and access controls for voice and data networks, verification of information security practices applied by digitally-connected business partners, and new controls on access to digital process control systems at our facilities."

Cyber review elements may include:

- Assess Cyber Security Vulnerabilities
- Implement Security Measures to Address Vulnerabilities
- Provide Training and Guidance to Employees on Cyber Threats
- Conduct Periodic Exercises to Test Cyber Security Systems
- Work With Designated Authorities to Share Information from Cyber Incidents
- Periodically Audit Cyber Systems to Identify Improvement Opportunities

How to Use This Information

Suggestions for using this material include but are not limited to the following approaches:

1) Read the NIST Cyber Framework.
2) Read the sector specific guidance (this document).
3) Create a plan unique to your company or facility to implement the NIST Cyber Framework and guidance. Creation of this plan could involve the following steps:
   a. Develop a scope that is manageable and leverage multiple iterations to accomplish success.
   b. Identify people and assets in your scope that align with your cybersecurity mission and describe specific missions.
   c. Identify the highest consequence assets, conduct a consequence analysis (e.g., a Hazard and Operability Study or HazOp[6]) focusing on your highest consequence assets and align with the appropriate tiers of the NIST Cyber Framework. The documented potential consequences and threats results of this step will be important to aid in determining the degree of investment and implementation you perform for each NIST category and guidance statement.
4) Identify the risk profiles and potential consequences to better define company risk tolerance, and review the NIST Cyber Framework sub-category by sub-category to identify gaps & opportunities relative to your current cyber security state and desired state through a review by sub-category of the NIST Cyber Framework. During the Tier selection process, an organization should consider its current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints.
   a. Define company risk tolerance through the application of the NIST Cyber Framework Profile concept.
   b. Identify the costs associated with achieving the desired cyber security state and a ranking of importance in alignment with the company risk tolerance definition.
   c. Obtain the necessary support to fund and close gaps.

[6] http://en.wikipedia.org/wiki/Hazard_and_operability_study

5) Based on asset consequence and company risk tolerance, set a frequency of refreshing the consequence analysis and the NIST Cyber Framework Profile.

Considerations

There are several items to consider when applying the above procedure:

- Look for suitable ICS related and Corporate IT tools and principles that can be shared within your organization on priorities (consequences vs. availability) and culture.
- Physical security is a layer of defense for both ICS and Corporate IT cyber and should be incorporated into your plan.
- Other groups (e.g., audit, business finance, operations management, Information Technology, physical security, etc.) need to understand the real consequence of failure or compromise of an asset. Consider sharing of principles between core groups like operations management and global IT while looking for similarities to add value to each group (e.g., philosophies for plant alarm management and cyber monitoring, change management, etc.).

Guidance by Function

The following guidance is provided for each of the functions contained in the NIST Framework. References to the specific section of the Framework are provided at the beginning of each step described below:

Identify

- (ID.AM) Develop an asset inventory that documents the potential consequences of an asset's failure or degradation. (e.g., an inventory of ICS and supporting devices and up to date network drawings to support incident response and risk mitigation activities)
- (ID.AM-2) Your inventory should include all system and application software, as well as level of code running. (e.g., degree of inventory must support vulnerability and threat analysis and recovery requirements; what software is used, where is it being used, and how is it being used?)
- (ID.AM-3, ID.AM-5) Document all information flows that directly support the business process and the consequence of failure in order to know the purpose and to support proper control configurations (e.g., isolation solutions, access limits, supply chain management- consider raw material thru delivery, etc.).
- (ID.AM-4) Identify and document all connections to other systems or parties. (e.g., HVAC, utilities, vendor, customer, etc.). Each should be described in terms of who is using it, for what purpose and when it is needed.
- (ID.GV-3) Identify applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance (e.g., Responsible Care Guidance, Data Breech, SOX, PCI, C-FATS, Data Privacy, MARSEC, etc.).
- (ID.GV-3, ID.AM) Asset Management should support applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance (e.g., Responsible Care Guidance, Data Breech, SOX, PCI, C-FATS, Data Privacy, etc.).
- (ID.GV-2, ID.AM-6) Establish Cybersecurity roles and responsibilities (e.g., employees, third-party stakeholders, suppliers, customers, and partners) for your company. Consider incident management, contingency planning, system administration, etc.

- (ID.BE-3) Identify business requirements for your assets, specifically considering your needs for the asset's confidentiality, integrity, and/or availability. Document these requirements in the asset inventory.
- (ID.GV-2, ID.RM-1) Identify appropriate governance and risk management accountability to address cybersecurity risks (e.g., clear roles and accountabilities).
- (ID.RA-1, ID.RA-5) Identify, assess and document asset vulnerabilities.
- (ID.RA-2) Gather and analyze threat and vulnerability information from information sharing forums and sources (e.g., US-CERT, ICS-CERT, Chemical Sector ISAC, system vendors, etc.).
- (Industry Experience- Not included in NIST framework) Include both physical and environmental consequences in the analysis of Cybersecurity risks.
- (Industry Experience) Identify and prioritize risk responses based on potential consequence.
- (ID.RM-1, ID.RM-2) Establish a consistent Risk Management process with all appropriate roles understanding consequence and agree to the process. Stakeholders include Environment Health and Safety, production operations management, Information Technology, physical security, and business management.
- (Industry Experience) For US operations, if required by regulation, perform a CSAT top screen for CFATS for each of your applicable sites.

Protect

- (PR.AC-2) Establish timely removal of physical access and disabling personnel accounts upon separation.
- (PR.AC-4, PR.AC-3) Review physical and logical cyber access including remote access, and limit based on consequences. Consider least privilege and segregation of duty principles where appropriate.
- (PR.AC-5) Based on consequence, establish a Zones and Conduits model[7] to segregate corporate business activities, plant floor activities, safety systems, etc. and manage access appropriately.
- (PR.AT) Establish appropriate role-based security-related awareness and training. Retain adequate documentation to support regulatory requirements (e.g., CFATS, MARSEC, CT-PAT, etc.).
- (PR.AT) Identify and provide access to available cyber security awareness training to leverage your program.
- (Industry Experience) Consider creation of a specific list of "Do's and Don'ts" that apply to your company; for example; a list could include don't charge cell phones from an ICS computer.
- (Industry Experience) Emphasize that information is an asset that must be managed. (process logic to run the plant)
- (PR.DS-1) Manage information and records (data) in a manner that is consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information. Keep in mind that the relative ranking of confidentiality, integrity, and availability varies (ICS focus availability and integrity, business IT focus on confidentiality, etc.)
- (PR.DS-2) Consider transmission protection to include but not be limited to reading data, altering data, and signal availability contingency planning.

[7] The methodology for developing this type of model is detailed in the ISA-62443 series of standards.

- (PR.DS-3, PR.IP-6, PR.IP-11) Erase or sanitize information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse. Employ mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.
- (PR.DS-5) Based on data security requirements, consider data loss prevention technology or other mitigating controls.
- (PR.IP-11, PR.PT-3) Establish employee and non-employee staff screening practices and consider rescreening requirements for high-risk roles.
- (PR.DS-2) Consider encryption for network communications beyond your physical security control when highly sensitive data is transmitted on the connection (e.g., fiber runs, microwave, raw internet, etc.).
- (PR.AC-5) Limit or eliminate direct connection without isolation or other protection safeguards of systems (e.g., Industrial Control Systems, HVAC, smart energy grid management, vendor management systems, building management, IP-Cameras, etc.).

  Reference: https://ics-radar.shodan.io/?utm_content=buffer3c996
- (PR.IP-3, PR.IP-9, PR.IP-10) Establish formal change management procedures for all devices considered part of the critical asset scope (e.g., ICS, firewalls, supporting IT systems, etc.). Consider that a change should not surprise the plant operator. Cover data work flow and consequence documentation in your principles of change management practices.
- (Tiers) Based on your designated NIST Cybersecurity Framework implementation tiers, consider controls for all critical information systems servicing Industrial Control System (e.g., consequence analysis, plant data management, active directory, Enterprise ERP, etc.).
- (PR.AT) Consider the importance of standards and principles with education to employees to make language clear to both operational management (ICS) and enterprise IT (services and assets). Consider joint or clear understanding of strategic plans and goals with key personnel (e.g., relationships between roadmaps for Operational Management for ICS, IT network, etc.).
- (ID.RA-5) Consider in your consequences and defense-in-depth strategy the need to cover many types of threats (e.g., supply chain threats, loss of containment of chemicals of interest, the chemical sector and your company’s role as supplier to critical infrastructure, etc.).
- (PR.DS-4, PR.IP-4) Give special consideration for continuous operations, including natural disasters (e.g., hurricane, earthquake, wild fires, etc.), and consider off-site backup location accessibility and not susceptible to the same natural disaster.
- (ID.GV-2) Consider industry sector opportunities with DHS via the American Chemistry Council and internal drills or table-tops to test and exercise your company's incident response capabilities (e.g., CyberStorm, NLE, corporate crisis drills, etc.).
- (Industry Experience) Although identifying technical vulnerabilities within the operating environment is important, organizations should exercise caution, particularly when performing scans of control systems.
- (PR.PT-2) Consider the acceptable use and mitigation procedures for removal media use, especially by vendor standard work requirements (e.g., USB stick for vendor patching and service work).
- (PR.AT, PR.PT-3, PR.IP-11) Consider the system or person that grants access (e.g., IT). The authorization to have access should come in advance from the owner of the asset, process or information, with clear roles and accountability for the asset, process, and information owner.

- Verify that the owner is close enough to assess and understand the consequences and details to fill the role effectively.
- (PR.MA-2, PR.AC-2) Consider remote access restrictions (e.g., employees or contractors, vendor support requirements, etc.). For external vendor support, consider processes that require internal actions prior to vendor connection to cause ushered access similar to safety physical access requirements.
- (PR.IP-9- ID.RA-4, ID.GV-2) Identify the top consequences for your company and consider for these events an incident response plan. The plan should include procedures to share incidents internally and externally (e.g., Sector ISAC, DHS, ICS-CERT, FBI, local emergency response, etc.), and under what criteria and to what level of detail information will be shared.

Detect

- (DE.AE) Consider logging configurations and anomaly monitoring practices to feed your incident response process for timely action. Understand the goals and objectives of logging and monitoring (e.g., detecting potential issues vs. criminal prosecution).
- (DE.CM) Consider implementation issues with advanced monitoring practices like continuous verified proactive measures and working closely with your ICS vendor to get appropriate guidance in your implementations (e.g., system hardening, malware, monitoring, etc.).

Respond

- (RS.AN, RS.MI) Analyze, contain/mitigate incidents in accordance with your developed response plan.
- (RS.RP) Consider your response plans to include the examination of cybersecurity events in the context of potential consequences beyond enterprise IT into ICS and vice versa.
- (RS.CO) Consider the value of timely reporting threat intelligence to sector information sharing entities within ACC and government cyber response agencies to insure full picture response. Consider building this practice into your incident response plans.
- (Industry Experience) Consider the sufficiency of resources to defend your operations technology and Industrial Control System. These resources may be available through a third-party, including the Department of Homeland Security's ICS-CERT. DHS has agreements available to safeguard the confidentiality of your information, including exclusions to the Freedom of Information Act, as well as the Protected Critical Infrastructure Information Act of 2002.

Recover

- (ID.AM-5) As part of your asset tiering and consequence evaluation, consider the effects on supply chain should the asset be out of operations (e.g., do you have a backup supply viable for the critical customers).
- (ID.AM-6, PR.AT-3) Consider that third party and vendor systems could be compromised (e.g., you may find the compromise before they do) and preplan in your incident response procedures, legal non-disclosure language, and who and how to communicate internally and externally for these type of events.
- (RC.IM) Consider reviewing guidance to identify additional elements or points to modify in your recovery plan.
- (RCCo3) Participate in information sharing forums within the chemical sector (lessons learned) to reduce future incidents.

Annex – Definitions

Consequence

Consequence, or impact, is the effect of an incident, event, or occurrence, whether direct or indirect. In homeland security risk analysis, consequences include (but are not limited to) loss of life, injuries, economic impacts, psychological consequences, environmental degradation, and inability to execute essential missions.

CSAT Top-Screen

Chemical Security Assessment Tool or CSAT shall mean a suite of four applications, including User Registration, Top-Screen, Security Vulnerability Assessment, and Site Security Plan, through which the Department will collect and analyze key data from chemical facilities.

Event

An observable occurrence in an information system that actually happened at some point in time

> Examples: Email, Telephone call, system crash, request for virus scans to be performed on a file or attachment

Incident

An adverse event in an information system or environment including the significant threat of an adverse event

> Example: violation of an explicit or implied security policy, the attempts to gain unauthorized access, unwanted denial of resources, unauthorized use, changes without the owner's knowledge, instruction, or consent.

Vulnerability Assessment

A **vulnerability assessment** is the process of identifying, quantifying, and prioritizing (or ranking) the **vulnerabilities** in a system.

Zones and Conduits Model

Zone and Conduits – Segmenting or dividing a system under consideration for the purpose of assigning security levels and associated measures is an essential step in the development of the program"

NIST Framework Definitions

The framework consists of three primary elements - Core, Framework Profiles and Implementation Tiers.

- **Core** - a set of cybersecurity activities using the following five functions that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk.
    - **Identify** - develop the organization understanding to <u>manage</u> cybersecurity risk to systems, assets, data and capabilities
    - **Protect** – develop and implement the appropriate safeguards to <u>ensure delivery</u> of critical infrastructure services

- **Detect** – develop and implement the appropriate activities to identify the occurrence of a cyber event
- **Respond**- develop and implement the appropriate activities to take action regarding a detected cybersecurity event
- **Recover**- develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

- **Framework Profile** – profiles are used to help the organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. As the organization's risk changes, so will the controls and processes.

- **Implementation Tiers** – levels of involvedness that the company is applying to its cybersecurity practices along with methods on how to apply to the core functions.

  - **Partial** – organization manages risk in an ad-hoc and reactive manner
  - **Risk Informed** – organization understands cyber security risk but lacks an enterprise wide approach to managing it
  - **Repeatable** – enterprises with a formal, integrated approach to cyber security
  - **Adaptive** – enterprise wide approach to managing cyber security risk that it continuously improves based on lessons learned and predictive indicators

Relevant Links

NIST Framework- http://www.nist.gov/cyberframework/
ACC Responsible Care Security Code- http://responsiblecare.americanchemistry.com/Responsible-Care-Program-Elements/Responsible-Care-Security-Code

"Responsible Care Security Code Implementation Guide: Site/Value Chain/Cyber", 2016

Revision History

Revision	Date	Description
1	2014-08-15	Initial draft
2	2014-08-29	First round of editing for clarity, structure and content
3	2014-09-17	Added legal notice
4	2014-10-27	Merged comments and revisions from the review process.
5	2015-05-07	Additional revisions.
6	2015-12-17	Revised based on peer review comments.