Recommended Practice:

Developing an Industrial Control Systems Cybersecurity Incident Response Capability

October 2009

Homeland Security

Control Systems Security Program

National Cyber Security Division

ABSTRACT

The strength, growth, and prosperity of this nation are maintained by key resources and a functioning and healthy infrastructure. Much of that infrastructure is sustained by a variety of industrial control systems. The term industrial control system refers to supervisory control and data acquisition, process control, distributed control, and any other systems that control, monitor, and manage the nation's critical infrastructure. Critical infrastructure and key resources consist of 18 sectors: Agriculture and Food, Banking and Finance, Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Government Facilities, Healthcare and Public Health, Information Technology, National Monuments and Icons, Nuclear Reactors, Materials and Waste, Postal and Shipping, Transportation Systems and Water. Simply stated, a control system gathers information and then performs a function based on its established parameters and the information it receives.

Industrial control systems, like traditional business information systems are coming increasingly under attack by a variety of malicious sources. These range from hackers looking for attention and notoriety to sophisticated nation states intent on damaging equipment and facilities. Included in this mix are disgruntled employees, competitors, and even friendly sources that inadvertently bring malware onto a site.

This document will present recommendations to help those facilities that use control systems better prepare for and respond to a cyber incident regardless of source. The document also suggests ways to learn from incidents and to strengthen the system against potential attacks. The document includes accepted methods and approaches from tradition information technology, but is primarily focused on the unique aspects of industrial control systems.

EXECUTIVE SUMMARY

This document provides recommendations for those interested in protecting industrial control systems (ICS) within a facility or organization. It is primarily focused on preparing for and responding to a cyber-related incident in which ICS are either threatened or compromised. It discusses ways of preparing for and preventing an incident as well as ways to respond, analyze, and recover from one should it occur.

The concept of incident response is familiar to most people in the context of emergency situations such as those caused by a natural disaster. The fundamental principles are the same in cyber incident response, including prevention, preparation, planning, incident management, recovery, mitigation, remediation, post incident analysis, and lessons learned. In cyber-oriented incident response, the focus is directed to negative events specifically caused by malicious parties using computers and related technologies. This document will not, for example, discuss physical security or non-cyber related issues.

This recommended practice narrows the focus even more to cyber incidents that are specifically directed toward ICS. Traditional information technology (IT) incident response has been defined for many years; however, related information and technology that addresses the unique considerations of ICS are only now emerging. ICS has some constraints that add complexity to the environment such as: the requirement to keep all key systems running despite of the fact that many systems are decades old and use unsecure protocols and architectures, the requirement to support nonstandard interfaces and protocols, and the challenge of maintaining equipment that may no longer have vendor support. This adds complexity in both preventing an ICS cyber incident and responding to it when it happens.

This document provides general recommendations for those having to manage incident response for the ICS. It is not intended to be a detailed examination of all actions involved in incident response but instead, this document attempts to provide references to sources that do go into more detail in the respective subject areas. The document will not elaborate on common approaches that are well documented in traditional IT references but will instead highlight and emphasize those areas that are unique to the ICS environment.

The document is divided into four primary sections. The first section focuses on planning for a cyber incident and includes establishing a cyber incident response team and setting up a response plan with appropriate personnel, policies, and procedures. The second section focuses on incident prevention. Incident prevention is especially important because it can reduce the seriousness of a cyber incident. The third section is incident management, which discusses four areas: (1) detection of potential or actual issues; (2) containment of the event, especially when related to malware installed on the servers; (3) remediation including eradication of the malware; and finally (4) recovering from the event and restoring the system to full functionality. The fourth and final section deals with post incident analysis, which includes determining the cause, access path, vulnerability, and other information necessary to better understand the incident as well as ways to prevent it in the future including cyber forensics and data preservation.

This document is to be used by asset owners that recognize the need for ICS-specific cyber incident response, including those interested in establishing response capabilities. It also can be valuable for those desiring to check their existing cyber response capabilities against the ideas presented in this document.

Because this document is limited in scope to address general recommendations, a suggested reading list, including cybersecurity best practice documents, is located at the end of this document. Recommended websites related to cybersecurity and incident response are also provided.

This cybersecurity incident response recommended practice is one of many recommended practices available to strengthen the security of ICS currently supporting vital processes throughout the critical infrastructure and key resource sectors of the United States.

CONTENTS

FIGURES

TABLES

ACRONYMS

AGA	American Gas Association
API	American Petroleum Institute
CC	Coordinating Center
CERT	Computer Emergency Response Team
ChemITC	Chemical Information Technology Council
CIAC	US DOE Computer Incident Advisory Capability – replaced by DOE-CIRC
CIDX	Chemical Industry Data Exchange
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRC	Cyber Incident Response Capability
CPNI	Centre for the Protection of National Infrastructure
CSET	Cyber Security Evaluation Tool
CSIRT	Computer Security Incident Response Team
CSSP	Control System Security Program
DHS	Department of Homeland Security
DOE	U.S. Department of Energy
ENISA	European Network and Information Security Agency
FIPS	Federal Information Processing Standards
FIRST	Forum of Incident Response and Security Teams
GFIRST	Global Forum of Incident Response and Security Teams
ICS	Industrial Control System(s)
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISA	International Society of Automation, formerly known as “The Instrumentation, Systems and Automation Society”
ISAC	Information Sharing and Analysis Center (May be associated with specific sectors)
ISO	International Standards Organization
IT	Information Technology
IT-ISAC	Information Technology – Information Sharing and Analysis Center

NCSD	National Cyber Security Division
NERC	North American Electric Reliability Corporation
NIAC	National Infrastructure Advisory Council
NIDS	Networks Intrusion Detection Systems
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
PIDS	Protocol-based Intrusion Detection System
RTOS	Real Time Operating System
SCADA	Supervisory Control and Data Acquisition
SP	Special Publication
U.S.	United States (of America)
US-CERT	United States Computer Emergency Readiness Team

KEYWORDS

Industrial Control Systems, Cyber Incident Response, Cybersecurity, Forensics, Incident Management, Incident Reporting, Intrusion Detection, Intrusion Prevention

Recommended Practice
Developing an Industrial Control Systems Cybersecurity Incident Response Capability

1. INTRODUCTION

The concept of incident response existed long before industrial control systems (ICS) or computers. The idea is based on preparing for and responding to unforeseen, negative events that may affect a business or organization. The cause of an incident may be unintentional, as in the case of a storm or flood, or intentional, as in the case of an intruder or vandal that breaks into a facility and steals or damages equipment or supplies. Regardless of the cause, it always has been a good practice to prepare for and appropriately respond to negative events affecting the organization. For years, industry has created contingency plans for events that have negative impacts on critical equipment or operations. For example, most asset owners have preventative maintenance programs, emergency backup power, and standby equipment. Only recently, however, incidents related directly to cyber threats against the ICS have faced asset owners.

Cyber incident response and cybersecurity are not new issues for traditional information technology (IT) organizations, but they are only now getting the attention of ICS vendors and asset owners. ICS has traditionally consisted of stand-alone systems that were isolated from many outside influences. Because of the convergence of technology, capability, and lower costs, these once isolated systems are frequently replaced or upgraded to newer, integrated systems that are linked across networks with common communications protocols and access points. This has the potential to directly, or indirectly open these systems to access from the Internet, exposing them to the same security vulnerabilities that have plagued IT for years. In spite of this increased threat, security awareness and effective policies and actions have lagged in the ICS area. Ironically, the need for quick and effective response to a cybersecurity incident may be greater in ICS environments than in traditional IT business settings, thus requiring different emphases and actions to be effective.

Standard cyber incident remediation actions deployed in IT business systems may result in ineffective and even disastrous results when applied to ICS cyber incidents, if prior thought and planning specific to operational ICS is not done. The speed and effective actions required to respond to an ICS cyber incident is directly dependent on the amount of forethought and planning that took place in advance of the cyber event. A great degree of preparation will be required of the cyber incident response team with the associated security plans, policies, and procedures established and practiced before the incident.

This document discusses what and how incident response should be conducted in the context of ICS, leveraging proven practices that have been applied in the traditional IT environment, and highlighting the differences. This document will recommend how to handle the unique challenges facing process engineers when dealing with cybersecurity and cyber incident response management.

1.1 Audience and Scope

This recommended practice was written for the team charged with creating a computer cyber incident response capability focused on protecting the ICS environment from cyber attack. This includes operations and plant managers, process engineers, security professionals, network administrators, legal, physical security, and other IT professionals. The team may be small in some organizations, where those involved may have varied responsibilities, or it may include a large group of specialists whose only job is to focus on a certain aspect of cybersecurity.

This document provides high-level guidance on how to develop a focused cyber incident response capability related to ICS with references and suggested readings for more detailed information. This is not a rewrite or a consolidation of available documentation on creating an incident response program in IT. A large body of excellent documentation already exists and is readily available. Rather, this recommended practice provides background information, best practices, and highlights considerations that need to be taken from proven incident response programs to be applied to the unique issues faced by the ICS cybersecurity team. The content is not technical, but a basic understanding of IT architecture and practices as well as ICS environments is expected. The ICS in this document are defined to include process control systems, Supervisory Control and Data Acquisition (SCADA), embedded systems, and distributed control systems. Other regulatory guidance documents also will mention Industrial Automation and Control Systems, which all will be called ICS in this paper.

This document does not replace specific sector standards, guidelines, and requirements related to cyber incident response. Some sectors require very specific and detailed incident response plans to meet compliance with the respective regulations; other sectors or industries may not. In either case, a cyber incident response capability should be established and implemented, leaving the specific approach to risk and implementation of the plan to the asset owner. This document provides assistance and guidance to those seeking to develop an incident response capability.

1.2 Background

Cyber incident response is the way in which an organization responds to a perceived cyber-related incident that may impact ICS owner assets or their ability to operate. An incorrect response may result in chaotic and reactionary actions that are ineffective or increase damage. Every organization should strive for a smooth, planned response with minimal impact to a company's operations. Accomplishing this will require plans and procedures that are in place and tested before a cyber incident occurs.

In the context of cybersecurity, including ICS, an incident typically entails unauthorized access to computer networks and equipment with actions resulting in some form of negative consequence to the asset owners. Damage might include stolen data, exposure of private or business sensitive information, interruption of key services, a shutdown of production operations, damage to physical equipment and the environment, and defaced public websites. The economic and social consequences of a breach could be quite severe when considering negative publicity, loss of customer confidence, potential lawsuits, and direct financial loss caused by interruptions in production operations or equipment replacement and repair.

The likelihood of a successful breach into any organization's computer networks, including ICS, is high for all systems directly or indirectly connected to an organization's business systems and/or the Internet. Many high profile companies and government organizations report thousands of access attempts each day. Attackers use a variety of techniques, such as reconnaissance, botnets, backdoors, social engineering, and hidden malware, to test cybersecurity vulnerabilities. Many attacks can be easily defeated by implementing basic security countermeasures such as properly configured firewalls, employee cybersecurity awareness training, and locked doors. It can be very difficult to protect against a highly experienced hacker or intruder. Even less-sophisticated hackers can quickly penetrate systems in the timeframe between when a new exploit is introduced and when vendors distribute patches to fix the exploited vulnerability. The timeframe between the vendor releasing a patch and an ICS owner applying the patch also introduces additional opportunity for even unsophisticated attackers.

In the world of ICS, this can be of even greater concern as patches may require extensive compatibility testing before deployment because of their critical nature and potential impact on operations. Such patches may not be quickly developed by the vendor, assuming the product is still

supported, or they may be delayed by months due to extraordinary testing requirements or limited demand.

As one considers the potential for some form of incident to occur, combined with the possible impact to the organization, it becomes clear that an incident response capability to consider these specific ICS concerns is needed.

A cyber incident response capability must include several elements that are proactive in nature to prevent an incident or better allow the organization to respond when one occurs. These elements are green in Figure 1 and include planning, incident prevention, and post-incident analysis/forensics. Other elements center on detecting and managing an incident once it occurs. These are reactive in nature and are typically carried out under severe time constraints and great visibility. These elements, shown in red in Figure 1, include detection, containment, remediation, and recovery and restoration.

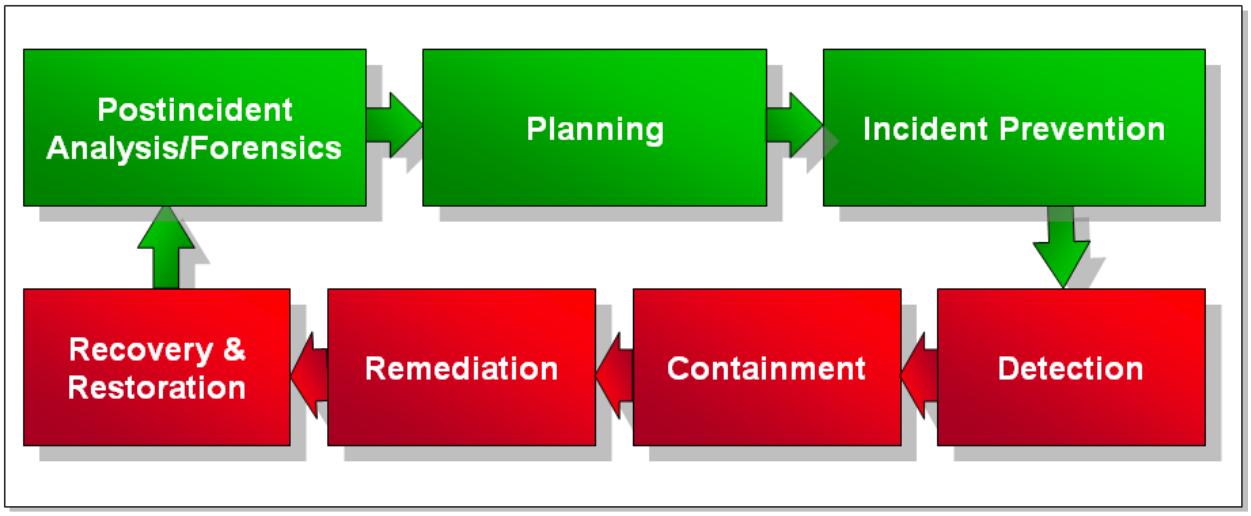

Figure 1. Incident response key elements.

To assist in the creation of an effective incident response capability, existing guidance documents that are available from established incident response organizations should be acquired and reviewed. These can be evaluated to determine what applies to the specific mission or charter for this organization. A large amount of information available is concerning how to develop a computer incident response team. Guidance documents from the United States, United Kingdom, and the European Union as well as sector specific documents (gas, oil, energy, nuclear, and chemical etc.) are readily available at little or no cost. The recommended reading section located at the end of this document and on the source websites lists examples. Here are a few resources from other well known CERT programs that may help in establishing a CERT baseline capability:

The U.S. Department of Homeland Security (DHS) Control Systems Security Program (CSSP) has developed the Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT), which is chartered to reduce control system cybersecurity risks within and across all critical infrastructure sectors. This program works in coordination with Department of Homeland Security created the United States Computer Emergency Readiness Team (US-CERT) with regard to cybersecurity but with an ICS focus. Supporting the ICS-CERT are expert staff that are familiar with vulnerabilities, intrusion techniques and tools, and methods to prevent or mitigate ICS incidents. They are current on cyber attack methods and preventive techniques. In addition, the CSSP provides products and services to reduce security risks to ICS asset owners. Other products and services include recommended practices, self assessment tools, ICS security documents, procurement recommendations, and standards support.

CSSP information can be found at website: http://www.us-cert.gov/control_systems/index.html.

Since the creation of US-CERT in 2003, their mission is to provide response support and defense against cyber attacks for the Federal Civil Executive Branch and information sharing and collaboration with state and local government, industry and international partners.

The U.S. Department of Energy (DOE) created the Computer Incident Advisory Capability (CIAC) in 1989, shortly after the Morris Worm appeared. Its mission was to provide various computer security services free of charge to DOE employees and contractors (reference "Assessing the CIAC Computer Security Archive," CIAC-2302 R.1). This mission has now migrated to the new DOE-Cyber Incident Response Capability (DOE-CIRC) with the charge to provide DOE with incident response, reporting, and tracking. This information is available to non-DOE entities.

US-CERT and DOE-CIRC are members of the Government Forum of Incident Response and Security Teams (GFIRST) and the Forum of Incident Response and Security Teams (FIRST). GFIRST is a group of technical and tactical practitioners from security response teams responsible for securing government information technology systems.

The Centre for the Protection of National Infrastructure (CNPI), which incorporates the former National Infrastructure Security Co-ordination Centre, publishes cyber-security-related guidance documentation for the United Kingdom. It is coordinated by the European Network and Information Security Agency (ENISA), which is an agency of the European Union, and is the Centre of Expertise for European Union member states and European Union Institutions in Network and Information Security. The Centre is charged with giving expert advice and recommendations on best practices for European Union member states, private business and industry. Best practices for setting up Computer Security Incident Response Teams (CSIRTs) in these organizations are listed in the recommended reading section of this document.

The National Institute of Standards and Technology (NIST) has developed several guides and publications addressing cybersecurity in general and incident response in particular. Recommended readings at the end of this document mention general guides and special publications; however, several specific documents on incident handling and response include:

- NIST SP 800-40, "Creating a Patch and Vulnerability Management Program"
- NIST SP 800-61, "Computer Security Incident Handling Guide"
- NIST SP 800-83, "Guide to Malware Incident Prevention and Handling"
- NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response"
- NIST SP 800-92, "Guide to Computer Security Log Management."

While these documents have a traditional IT orientation, they provide guidance for implementing ICS incident response policies and procedures as well.

In addition to government resources, numerous private sources of expertise on incident response are available. These include colleges and universities, hardware and software vendors, private organizations and institutes, consulting firms, and individual experts. An IT-oriented example from Carnegie Mellon Software Engineering Institute is the *Handbook for Computer Security Incident Response Teams (CSIRTs)* by Carnegie Mellon University.

2. CYBER INCIDENT RESPONSE PLANNING

The beginning point for creating a cyber incident response capability is the planning and preparation phase. All the elements are brought together to prevent an incident if possible or to be ready to respond to one if it occurs. The sections that follow will explain this phase, as shown in Figure 2.

A cyber incident response capability consists of several core building blocks that include the organization of the response team, establishing the organization's policies and procedures, developing the response plan itself, defining reporting and communications within and external to the team, verifying that the plan works as expected, and then enabling state and status reporting to support the team if and when an event occurs.

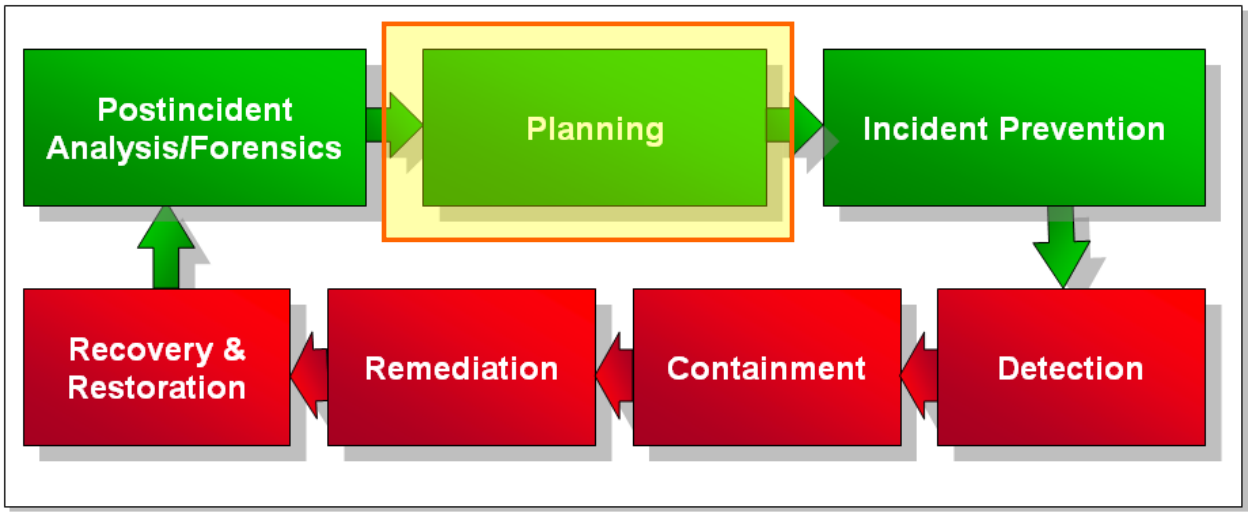

Figure 2. Preparation or planning phase.

2.1 Organizing the Team

The first step in developing an incident response capability is team organization. Most groups are organized into what is typically called a CSIRT. The CSIRT may be composed of specialists dedicated to this effort or part-time staff with other day-to-day responsibilities. In this document, the CSIRT will refer to the *internal* response team that is directly supporting the ICS. Other external response teams are organized around specific technical areas or along geographical or organizational boundaries.

2.1.1 Team Responsibilities

The responsibilities of the CSIRT will vary depending on the asset owner's organizational size and structure. The responsibilities also may be shared among different departments that have not traditionally provided support to the ICS security team. Third party involvement can be used through vendor service level agreements with equipment vendors or with consultants or other specialists. This option may be necessary for asset owners with limited resources.

The cyber incident response team's responsibilities will include:

- Acting as an expert resource on cybersecurity threats and vulnerabilities
- Serving as a clearing house for incident prevention, information, and analysis
- Developing organizational policies and procedures related to incident response

- Understanding safeguards on the ICS
- Identifying operational impacts to the organization in the event of an incident
- Creating and testing the incident response plan
- Acting as a single point of contact for all internally reported incidents or suspected incidents
- Responding to the incident when one occurs
- Reporting to key stakeholders and external agencies after the incident such as ICS-CERT and law enforcement
- Gathering forensic information to support analysis and any legal actions
- Implementing safeguards to prevent a recurrence of the incident
- Remediating the ICS after the incident.

2.1.2 Team Organization

Various models[a] have been identified for organizing a CSIRT. The most applicable CSIRT model for ICS environments is either a centralized or a distributed response team.

A centralized cyber incident response team may be found in various size organizations and is made up of individuals with various backgrounds. Its distinguishing feature is the close geographic proximity to the ICS. In this approach, servers, networks, monitoring equipment, engineering workstations, and the controlling devices connected to physical equipments are all typically found at one facility. This single team works on site and handles all the incident response activities. This model is the recommended approach, where possible, because it will reduce the overhead associated with multi-team interaction and allow for onsite access, control, and analysis.

A distributed response team may include a central CSIRT, but because of the separate physical location of the organization, multiple teams may exist or be required. This model applies where facilities are spread across multiple states, or even countries and a single team would not be able to respond in a timely way to any specific incident. It is also necessary in large organizations that are geographically dispersed, where the remote teams may include contracted specialists or even part-time staff. This approach requires more emphasis on communications and coordination between teams, but it also allows for a remote team to be onsite at the source of the incident. It is recommended that distributed organizations have strong centralized CSIRTs with self-contained, individual CSIRTs in the remote locations. Planning, prevention, analysis, and forensics can all come from the central group, allowing for efficiencies of scale. Incident response, however, must be a hands-on experience with the local CSIRT taking the lead on an incident, with the support of the organizations central staff.

Although this document does not address staffing issues, there are several excellent publications available that go into greater detail on this subject.[b] Even so, a couple of key ICS-related issues must be addressed when organizing the response team.

- IT environments undergo dynamic change with commonality in network configurations, operating systems, and equipment. By comparison the ICS environment tends to have static configurations and

---

a. More information about CSIRT models is provided in the Carnegie Mellon University handbook titled “Organizational Models for Computer Security Incident Response Teams (CSIRTs),” December 2003, Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek.

b. For more information on the staffing models, see NIST Special Publication 800-61, “Computer Security Incident Handling Guide,” January 2004, pp. 2.82.16.

Also see the above noted CMU handbook for the CSIRTs mentioned above.

typically consists of unique and even deprecated devices with site/operations-specific configurations. When dealing with a common piece of ICS equipment, its use, and the impact as a result of failure is almost always unique to the particular organization. Unfortunately, this environmental knowledge is often limited to a few key control systems engineers. This aggravates the problem of attempting to provide continuous coverage with a limited pool of resources. If allowed to continue, it can result in employee burnout and higher turnover, both of which are detrimental because specialized knowledge is needed to maintain and operate these systems. In organizing the team, consideration must be given to assignments and may include delegation of as many tasks and responsibilities to non-key staff, or to subcontractors, as possible.

- Staffing decisions must address division of authority. In IT, decisions typically roll up to a chief information officer (CIO), IT director, or equivalent. ICS operational responsibilities will often fall on the plant manager who is highly sensitive to interrupting the process. The plant manager also may come from a traditional engineering background and not have adequate awareness of cybersecurity issues. Upper management may pressure the plant manager to prevent any work stoppage. An understanding, with agreed upon authority must be established between the CSIRT, operations, engineering, and IT management prior to an incident. Each of these organizations can bring important knowledge and skills to the team, but the CSIRT must have the proper level of authority from the beginning, otherwise, valuable time will be lost determining authority while plant operations are at risk.

2.1.3 Staffing Roles

Though every organization will not be able to staff each position directly, each role should be identified and assigned, even if it is part-time, with staff having multiple roles, or with personnel from the ICS integrator or ICS vendor/manufacturer. For larger organizations where the demand might be greater, or to ensure redundancy, it may be necessary to have several people assigned to a particular role. This is especially true for process and operations engineers with unique knowledge and experience. Each CSIRT role is described as follows:

- *CSIRT Team Manager.* It is necessary to assign one person the responsibility of seeing that the team is organized and accomplishes its objectives. This person may act as a technical lead, or a separate technical lead may be designated from someone on the CSIRT. The manager should have the authority granted by senior management to act in the best interest of the company. If functions of the CSIRT are outsourced, then this person must oversee the actions, tasks, and contracts of subcontractors. This person is critical to assembling key resources to mitigate, contain, and resolve computer incidents in a timely and successful manner.
- *Process or Control System Engineer*. This person should be the subject matter expert on the control system architecture and should know and understand the system components and products being produced or supported by the ICS. He or she provides important information on normal and abnormal equipment functions and functional cycles as well as the potential impacts when a component in the ICS is removed from service. The process engineer is key player to the CSIRT's understanding how to resolve or work around equipment failures and how to resume operations when necessary.
- *Network Administrator.* The network administrator can provide a key role in the CSIRT if the incident involves a cyber attack originating from the computer network. This person typically should be knowledgeable on network access, including security vulnerabilities, patching, intrusion detection, and system monitoring. Knowledge and availability of activity logs from network switches, routers, and firewalls before, during, and after a cyber event are crucial in determining the scope and complexity of the incident and provide insight on how to resolve and remediate any vulnerability discovered. Most cyber related incidents will involve a network, and thus a knowledgeable network administrator is the key to finding and resolving an incident.

- *System Administrator*. This is primarily the control system administrator, but it also may include IT administration because of the high degree of integration in modern organizations. The system administrator should be knowledgeable about the access permissions and system operation logs on affected servers. Administrators may be familiar with process control operations and operational cycles. These administrators should be aware of what is happening on their respective systems and should be cognizant of potential vulnerabilities. They also may interface with vendors and suppliers.
- *Plant Manager (including ICS and Control Center Managers)*. While this person may not be involved in many of the details of the incident response plan, the plant manager must be involved in assigning authority to interrupt operations, being part of the risk assessment process when an incident is identified, funding CSIRT tasks, and acting as a liaison to executive management and external parties, including the press.
- *IT Director, CIO, or Chief Engineer.* This role is similar to the plant manager in terms of responsibilities. These two management positions are essential and must communicate and coordinate delegation of authority and what resources can and will be applied to an incident. A modern control system is typically integrated into existing IT networks, business systems, and communication equipment.
- *Security Experts.* Security expertise may include physical security and law enforcement, but in the context of this paper it deals primarily with cybersecurity expertise. These individuals may play dual roles, but someone needs to be available with in-depth knowledge of vulnerabilities, exploits, prevention techniques, and especially an understanding of how to prevent incidents and how to recover if they occur. They also may, on occasion, be involved in supporting identification and prosecution of criminal activities.
- *Legal Experts*. Legal expertise is necessary in several areas including: ensuring compliance with all national, international, federal, and state laws and regulations; explaining what evidence is admissible when taking action; specifying how evidence can be collected; third-party maintenance liability exposure; and helping the team understand what pitfalls, such as privacy rights violations, should be avoided. These individuals can be very useful when the team is preparing the incident response plan, enabling state and status reporting, and in forensics and data collection. Larger organizations may have legal departments in house. Smaller organizations may require outside legal help, in which case, legal firms should be contacted that have had specific experience with incident response issues.
- *Public Relations Specialist.* This person should be involved as necessary. He or she will play a critical role if the incident causes noticeable disruption to service or impacts the organizations ability to deliver a product. This can be especially important if the organization supplies services directly to the public, such as in the generation of power or treatment of waste water. This person is responsible for ensuring the appropriate information and messaging is sent to the public via the news media.
- *Human Resources Specialist.* The human resources specialist will be involved in CSIRT activity if the incident is being attempted or carried out by someone inside the organization. Legal issues, policies and procedures, and punitive actions will typically be handled by this person.
- *Vendor Support Engineers*. Because of the specific and essential knowledge held by the vendor's technical staff, individuals from the vendor facility should be identified that can provide technical support to the asset owner on the equipment and systems involved in the incident. These individuals can provide information and understanding that may not be found in the CSIRT. For example, their expertise would be valuable in restoration of the asset and also for the creation of custom patches, if necessary.
- *Other Support Staff*. Support personnel can be added to the CSIRT as additional expertise is needed. These could include legal or law enforcement personnel, computer forensics specialists, risk

management specialists, database administrators, application developers, platform specialists, and governmental agencies if warranted. For daily tasks like organization support and scheduling or preparing policies and procedures, secretarial and technical writing personnel are valuable.

If the CSIRT model is distributed, as many of the above-mentioned roles as possible, should be filled at the central office with specific technical staff available at each remote location. At a minimum, someone with process engineering, system administration, and network experience should be available at each distributed location. Communications must remain effective and reliable when an incident occurs, recognizing that the incident itself may disrupt normal communication paths.

Logistical elements will not be discussed at length, but recommended infrastructure for the team would include some type of permanent or temporary "war room," mobile communication devices, laptops, and available documentation, including policies, plans, procedures, phone lists, etc., all residing in locations that are less likely to be compromised by an incident.

While the primary focus of the CSIRT is to handle cyber-related incidents, the response team could be used for non-cyber events such as ICS or SCADA system outages, catastrophic equipment failure, or natural disasters such as floods or hurricanes.

2.2 Setting Policies and Procedures

While having policies and procedures are important in most business functions, incident response is important because decisions are being made under pressure of production stoppage, high financial cost, often at the most inconvenient times, and in situations where those with authority may not be readily available. Development of procedures and supporting policies while team members are not under pressure is crucial. At that time, team members can discuss and weigh options, test the approach, analyze impacts and alternatives, and obtain management input and approval. Many types of general cybersecurity policies[c] are valuable for both IT and control systems protection. In the context of this document, policies related to incident response should be established and published within the ICS organization.

Clearly written, detailed operating procedures should be developed to implement the incident response policy. The procedures found in an incident response plan are similar to those found in non-cyber emergencies and should be tested before the event occurs. Problems in the mechanics, accuracy, and timeliness of the procedures should be discovered during the development phase, when adjustments can be made, rather than in the middle of an actual response.

The initial incident response policy should direct the establishment of the CSIRT and lay the foundation for the incident response plan. The incident response plan should define the authority of the CSIRT. The policy will be the backbone for the procedures and actions defined in the plan. Although many additional security-related policies exist that should be considered, those that relate more directly to ICS are as follows:

- *Human Resources*. Policies should be included that address actions taken against employees or contractors when the incident is caused by someone inside the organization. These would apply to immediate response and actions during a discovered incident, how the investigation is conducted, and any related punishment policies.
- *Information Disclosure.* Policies must be defined to address the organization's position on disclosure, and what actions it will take in the event of an information breach. Policies should include who to contact and what time constraints exist on reporting. The plan must address information that may be

c. Examples of general security policies would include policies on: acceptable use, passwords, backups, remote access, wireless access, guest access, encryption, data classification, retention, and VPN policies, among others.

stolen and potentially sensitive. This may include security classification levels, private personal data, business or engineering process information, or even vendor proprietary data or code that may reside on a control device.

- *Communications*. If an incident occurs, policies should be in place regarding media interaction and communications. The policy should define who will speak on behalf of the organization. It also may define interaction with vendors and customers.
- *Authority Assignments*. As mentioned earlier, in the control system environment, a tendency exists to have dual organizational responsibility. The plant manager is responsible for operations, and the CIO is primarily concerned with the networks and computer-related equipment connected to or even used in the ICS. Policies should address escalation lists and division of authority as well as delegation, including backup, when a specific manager is not available.

2.3 Building the Cyber Incident Response Plan

The cyber incident response plan establishes and documents the procedures and actions that implement the incident response policy for the ICS. It defines the security incident and outlines the steps that should be taken to respond to the incident and mitigate damage to the organization. A variety of IT-related incident response plan templates and examples are available, some of which are included in the references. They can serve as a good starting point for building the plan. The following key sections should be considered when creating the plan.

1. *Overview, Goals, and Objectives*. These sections of the plan define what will be accomplished. In these sections, the organization can provide direction and guidance for overall business objectives in comparison to the response options to the incident.
2. *Incident Description*. Many IT-type incidents are fairly easily classified. These include denial-of-service attacks, unauthorized access to networks, accessing protected and private information, defacing web pages, misuse of services, etc.

   In the ICS environment, clear definitions of what is a security incident must be identified and communicated to the extent possible. This is particularly important when considering if equipment failure or unexpected software behavior is caused by a cybersecurity incident, due to mechanical failure because of wear, environmental conditions, or other non-security related factors. It is important to understand and differentiate between a cybersecurity and non-cybersecurity incident. If an isolated case of equipment or software failure exists, a replacement may resolve the problem. If the failure is the result of a compromised vulnerability, corrupt or untested patch deployment, or if malware remains somewhere on the system or network, then the original or other similar equipment may be at risk. Replacing the hardware or software will not resolve the problem or prevent re-infection if the configurations are the root cause of the incident. Accurate descriptions of an incident will also prevent unnecessarily activating the CSIRT.

   With ICS, differentiating between cyber-based incidents and those caused by other sources is critical. For example, the reaction to equipment damaged by a disgruntled employee with a crowbar would be vastly different than damage to the same piece of equipment caused by an unknown attacker who manipulated controls on the equipment. It's important to identify and define each incident type so that the appropriate response can be followed for that unique situation is important.
3. *Incident Detection*. This is also called "discovery" and includes ways in which an incident is identified and reported. While few cases of obvious incidents (an intruder is found logged onto the ICS network or a website is defaced) exist, detecting most incidents will require automated analysis tools, system behavior patterns, and an awareness of what to look for among operators, supervisors, and other staff. The operators and the process engineers are usually critical to detection of unusual

operations and are the first to note a difference in system behavior. This difference is the key to understanding what is happening in the ICS. The response plan must address automated systems, expectations for staff, contractors, and partners when suspicious activity is detected; and procedures for help desk and call center staff.

4. *Incident Notification*. Once an abnormal event is identified, it needs to be prioritized to determine the cause and whether this is a minor system event or if it requires immediate escalation. This section of the plan should identify the contact information for incident reporting. The section should include basic work phone, mobile phone, e-mail, instant messaging, and pager information for internal staff, including system and network administrators. It also should address the following circumstances:

    - After-hours phone and pager
    - Offsite contact numbers
    - Contact information for customers and partners
    - Phone or pager numbers for backup staff
    - Contact information for management and rules for escalation
    - Criteria for filtering out false positives
    - Contact information for any relevant regulatory authorities
    - ICS-CERT/US-CERT contact numbers and information
    - Vendor/integrator responsibilities and contact information

This contact information should be publicized to everyone that might identify a potential incident. A weekly and monthly duty call list issued to operations may be of help to let all employees know who is available to call for assistance in the event of a cyber incident. Because external agencies may be reporting a potential incident, based on events at other sites, the contact information should be available to all necessary external organizations as well.

5. *Incident Analysis*. Procedures in the plan should address how to evaluate and analyze a reported incident. The incident might be reported by internal or external sources and could happen at any time. In this stage of incident management, those receiving the report must determine:

    - What dangers or effects on the facility or facility personnel safety may be caused by the event
    - If the reported incident is real or a false positive
    - What stage the incident is in—beginning, in process, or has already occurred
    - What the impact might be to the organization
    - The specific type of incident
    - What systems and equipment are or may be affected by the incident
    - If the system has failed over to an available backup system
    - If the incident has the potential to spread across other networks or even outside to partners or customers
    - What organizations will be affected and who should be part of the response.

6. *Response Actions*. This section is essential to the plan because it defines the procedures to follow for each type of incident detected. An incident will typically occur at the most inopportune time; there will be increased stress and pressure on staff, little time for testing options, and every action will be watched and measured by upper management, stakeholders, and perhaps even by the public. It becomes essential that well thought out actions be defined and tested before the incident occurs. When defining the response actions, consider the following:

    - The response must be directly associated with the incident type; one approach will not fit all situations, and new attack vectors should be considered on a regular basis.

- The plan must account for contingency situations including nights, weekends, holidays, unavailable staff, and nonfunctioning communications equipment. External factors affecting the plan, such as deliberate or accidental power loss, also should be addressed.
- The actions identified in the plan must include a comprehensive response covering containment of the problem, restoration of operations to a functional state, and prevention of a reoccurrence. As mentioned above, the actions will be dependent on the type of incident and its severity.
- The response procedures should be tested in a situation as realistic as is practical to determine elements that were missing, misunderstood, incomplete, or inaccurate. Corrections can be made and then retested until all concerns have been addressed.
- The response actions must be weighed against business impact and approvals secured while in the planning stages. Some remediation activities may cause more harm to the business than the incident itself.
- All available perspectives should be involved in preparing the plan. This includes technical, legal, communications, management, operations, engineering, and human resources.
- The actions must take into consideration any forensics requirements. It will not be necessary in all cases, but some incident types will require that the procedures accommodate the need to identify and preserve information for potential criminal or other legal actions.

7. *Communications*. While elements of communications could be included in the response actions, the topic is unique enough that it could be addressed in a separate section in the incident response plan. The communications section should include:

    - Lists of all necessary contacts in the media, emergency responders, civil authorities, and local and global organizational contacts.
    - A designated point of contact with one or more alternates who are prepared to speak for the organization when an incident occurs.
    - Prepared and vetted statements and press release information that would be available for immediate use. This is particularly important when the organization provides a product or service on which the public depends.
    - Reporting chains both internal and external to the organization.
    - A current list of contact names with the respective skill sets at key vendors for critical systems and components in the overall ICS.
    - A description of alternate physical methods to handle impaired communications through the telephone lines, cellular networks, or the internet. This would include contingencies if any or all the methods were non-functional.

8. *Forensics*. Cyber forensics focuses on collecting, examining, and analyzing data related to an incident along with protecting incriminating evidence for use in legal action against a suspected offender. This data can be found in available logs (network, server, and workstations), physical components (hard drives and bitmap images of affected real time operating system [RTOS] if possible), emails, voicemail, texts, and telephone records. While the information gathering can be useful in understanding the incident and helping in preventing further actions, the approach has nuances related to data integrity and protection that go well beyond just learning about an incident. A recommended practice[d] is available that focuses completely on cyber forensics related to ICS. This recommended practice should be consulted when preparing the forensics section of the incident response plan.

d. See "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," August 25, 2008, Control Systems Security Program (CSSP), Department of Homeland Security. (See US-CERT website for document).

9. *Additional Sections*. The areas mentioned above are essential elements of the incident response plan. The plan may be divided into more detailed topics, if desired, and may include other sections, such as incident tracking and reporting, as necessary.

2.4 Exercising the Plan

Although it may be inconvenient and disruptive to plan for, conduct and evaluate the results from an incident response drill; considering the stakes involved, it is essential. Even the best response plans cannot anticipate all the obstacles that will be faced when a real incident happens, nor can they anticipate, in all cases, how people will react to unforeseen situations. The people who were expected to be available and fill certain roles will often be inaccessible. New people may have replaced previously trained workers. Unanticipated events may occur where decisions need to be made with little or no time for analysis.

Many problems that would occur in a real incident also will be present in the test exercise or drill. This means that an opportunity is available to review, analyze, and change the procedures without suffering the effects of catastrophic decisions or even lost production. This is only true, however, if the plan is tested in an environment closely replicates the production system.

To conduct partial tests of the incident response plan is also productive to evaluate unexpected behavior. These partial tests allow adjusting and making the plan more effective and streamlined prior to a full test. Partial testing can be a good training exercise for new Computer Incident Response Team members without incurring the cost and disruption of a full test.

The following are items that may be considered when setting up the incident response simulation.

- Some aspects of the incident response plan will be similar for all incident types, but others will be vastly different. Different incidents may require different levels of response, for example, an intruder scanning the ICS network but not altering equipment settings would require a lower level of response than someone overriding safeguards to lock up pumps or valves that control the processing of toxic chemicals. The drills should address as many critical scenario types as possible and the nature of the drill adjusted accordingly.
- The exercise should mimic real-world conditions as much as is practically possible in order to discover weaknesses in the incident response plan. The closer the exercise is to the actual circumstances of the operating environment, the more problems will be found and resolved before a real event occurs. Actual equipment should be used if possible in order to gain accurate insight into how the incident response plan plays out. This may mean working with a vendor to provide temporary equipment specifically for the exercise.
- The drill should simulate worst-case conditions. An intruder who is intent on causing the most damage possible or who is seeking widespread publicity may intentionally strike at the worst possible time. Depending on the desired outcome, this may be at the peak of the workday when the maximum numbers of people are on site, or it may be in the middle of the night on a weekend or holiday when key technical staff and decision-makers are gone.
- The drill should involve all those who may be involved in the response and mitigating efforts. Having trained one set of people will not be helpful if the actual workers that face the incident are not knowledgeable on what to do if an event happens on their shift.
- Drills should be held on a regular basis to accommodate staff changes, changes in the facility or equipment, and new information gained from previous drills and actual events.

- Circumstances surrounding the drill should be designed to cause the staff to think through unusual situations. This can reveal weaknesses in the decision-making process and potential unintended cascade effects and consequences.
- The CSIRT should, wherever possible, draw upon the experience of other facilities in preparing for the drills and potential incidents. This information can be found by working with the staff at the ICS-CERT and with the experts from the CSSP.

2.5 System State and Status Reporting

Enabling system state and status reporting refers to associating automated mechanisms with the hardware or software that report information about the system, including abnormal behavior, intrusion attempts, or any other data that would be useful in detecting an incident, understanding impact, and quickly supporting resolution. Examples include network logging and database auditing, customized applications developed in-house for specific networks or equipment, or vendor-developed capabilities built into supplied equipment.

When programmers apply state and status reporting to software applications (or build code into the program solely to provide status or state information unrelated to its intended purpose), it is almost always done to help in debugging the program or in providing support information if problems are reported. When considering justification for expending resources to enable the system, consider that it can be helpful for resolving any type of system problem, including debugging software, detecting pending equipment failure, or just improving efficiencies in the work processes.

Adding code to report state and status information can be very valuable in supporting forensics after an incident has occurred. However, its primary purpose is not forensics, but rather incident detection and resolution.

While there are real advantages to enabling status information about the ICS, challenges exist. Because of the nature of ICS, many devices are designed with volatile memory, the base code may be difficult to access. Vendors may be reluctant to add new code because of cost or risk. In addition, data that is generated and available is often replaced so quickly that log data cannot be written or stored in a practical way. Network traffic loads can be affected by the additional logging, even to the degree of altering or impairing normal operations.

A variety of ways to approach automating system components are available to collect useful information. Several key types of approaches are:

- *Networks Intrusion Detection Systems (NIDS).* These applications, which include both hardware appliances and software solutions, reside on the network and are useful in detecting attempts to access the network. They have been around for many years in IT and are equally useful in the ICS environment. A NIDS will act to alert the network administrator of intrusion attempts and record all alert information, according to parameters set by the administrator.
- *Protocol-based Intrusion Detection System (PIDS).* A PIDS is associated with a component rather than the network. Typically it would reside between a server and a connected device and analyze communication protocols between the two. A variation of PIDS is the Application Protocol-based Intrusion Detection System, which is placed between several servers, all communicating with application-specific protocols.
- *Host-based Intrusion Detection System (HIDS).* An HIDS resides on a host system and analyzes data unique to the applications on the host. It may include analysis of log files, file systems, database changes, etc.

- *Intrusion Prevention System (IPS)*. Because of the immaturity of IPS technology and the high risk of inadvertently causing ICS failure, these systems are not currently recommended for ICS environments. They are mentioned so-as to provide a more comprehensive understanding of available technology and for their potential role in integrated business systems. An IPS is similar to an intrusion detection system (IDS) with the exception that it actively reacts to malicious activity and blocks or prevents the activity if possible. If implemented in the ICS environment, both the NIDS and IPS will be most closely associated with the network with some limited application to server-type components. Detailed information is readily available on the internet for IPS and IDS-type products. Extensive preliminary testing to ensure ICS compatibility is highly recommended before system deployment. An active system like the IPS can prevent legitimate activity, so the establishment of approved activities is critical before this approach can be used.
- *Network and Device Logging*. Mature products are available on the market for network logging including the IDS types mentioned above. This is not always the case with the variety of control system devices being used. Device logging will vary based on age, vendor, device type, and available settings. Administrators should enable auditing and logging capabilities whenever they are available and in circumstances that will not interrupt operations. Vendors should also be encouraged to provide self-monitoring capabilities with new products or upgrades to existing hardware.
- *Configuration of Data Generators*. Several key elements should be considered when using commercial systems for successful data gathering. It is important to know and understand all settings, properly configuring the device, and regularly monitoring alert notifications. A perfectly operating detection system will be of no use if an alert is sent but no person receives or acts on the notice. This can be the case when a duty officer has not been assigned or when so many false positives are published that actual incidents may be easily overlooked. For customized logging and monitoring, having useful settings will increase the value of the device. For example, the state of field devices in normal operations may be measured and reported to a server on a constant basis. The server may have an ongoing test for out-of-range conditions or unusual traffic, which would be reported via e-mail, pager, alarms, etc. The key is to analyze the specific devices involved and apply either vendor-provided or custom-monitoring capabilities to the device. With custom monitoring, no direct access to devices may exist, especially those that are older or have proprietary software. In these situations, monitoring internal to the device may not be available, but there may be an opportunity to test signals going to and from the device. External ways to accurately validate the state and status of the component may be available. Differences exist between the ICS and business systems in regard to network traffic. Because ICS traffic is limited and specific, as compared with the business systems, signatures can be created based on what is outside of range or is abnormal after the baseline has been taken.

Take care when enabling state and status reporting on the ICS because some systems and applications have the potential to introduce operational issues.[e] For example, some legacy control systems can be disabled or shut down because of the very intrusive nature of some IDSs and antivirus tools. Poorly configured IDSs and antivirus tools have slowed critical data communications to the point the ICS becomes inoperable. Any plan to deploy these tools must be checked with the ICS vendor and tested for compatibility with the ICS and additional supporting applications that are co-resident on these systems. Some newer software may be incompatible with existing support software (various Java versions for example).

Questions regarding these types of systems include:

- Where will the log files be stored?

[e] CSSP strongly recommends that all methods within this document be thoroughly tested prior to production deployment.

- How long will the log files be stored?
- Will older log files be deleted or archived?
- What parameters are being investigated? (Ports, login/logout times, abnormal traffic cycles and times, etc.)

3. INCIDENT PREVENTION

Preventing a cyber incident is preferable to responding to one, but prevention takes on a whole new dimension in the ICS environment. This is because compared with typical IT, beyond the network there are far fewer, and in some cases, no detection capabilities available in system devices. In addition, working components may have vulnerabilities that may never be fixed, and the results of the most severe attacks could include injury, loss of life, and severe financial loss. Because the relative vulnerability and consequences are both high, the facility should put sufficient resources into incident prevention.

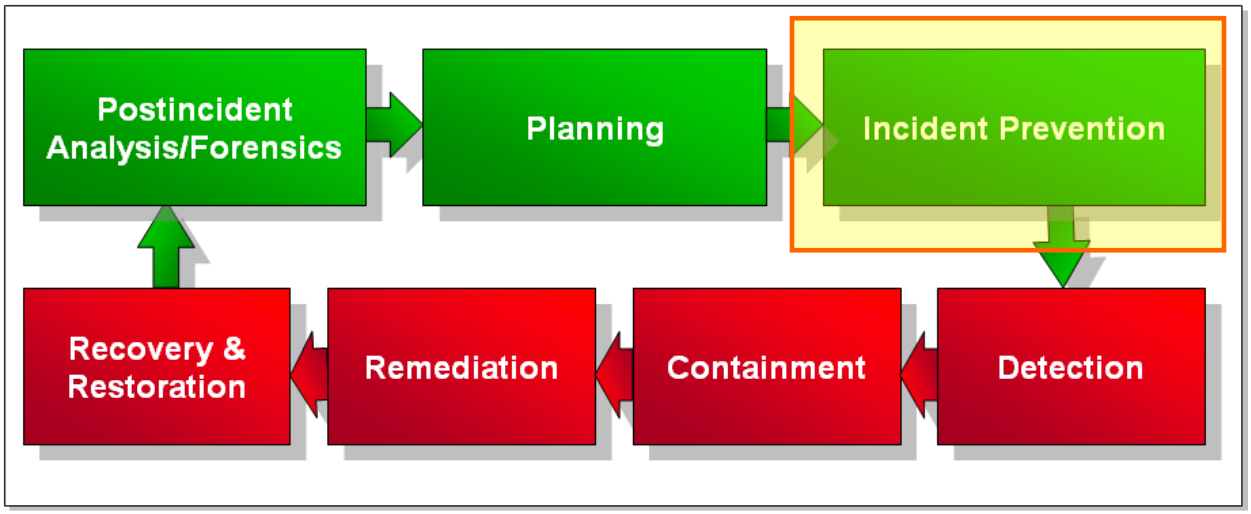

Figure 3. Incident prevention phase.

3.1 Tools and Guidelines

This recommended practice is one of many standards, guides, white papers, applications, and software tools that have been developed to help protect the ICS from cyber attack.

NIST developed two standards to assist in preventing cyber attacks on the control systems networks. SP 800-53, “Recommended Security Controls for Federal Information Systems — Information Security,” was developed for information systems in general and is effective in preparing the full security plan. Until recently, ICS had little resemblance to traditional information systems in that they were isolated systems running proprietary software and control protocols. However, as these systems have been increasingly integrated into mainstream organizational information systems to promote connectivity, efficiency, and remote access capabilities, they have started to resemble the more traditional information systems. To address this, NIST has worked cooperatively with ICS communities in the public and private sectors to develop specific guidance on the application of the security controls in SP 800-53 for ICS under Appendix I.

NIST developed SP 800-82, “Guide to Industrial Control Systems (ICS) Security,” specifically for the control systems environment. This document was in final public draft status at the date of this publication. Other standards and guides have been written for specific sectors using forms of ICS.

Appendix A of the *Catalog of Control Systems Security: Recommendations for Standards Developers*[f] provides the other standards in Table 1. These standards have been updated to later versions from those listed in the catalog, where applicable, and additional standards not found in the catalog have been added.

Table 1. ICS Security Standards.

Common Label	Description
AGA 12-1	American Gas Association (AGA) Report 12, "Cryptographic Protection of SCADA Communications Part 1: Background, Policies and Test Plan," March 2006.
AGA 12-2	AGA Report 12, "Cryptographic Protection of SCADA Communications Part 2: Retrofit Link Encryption for Asynchronous Serial Communications," March 2006.
ANSI/ISA-99.00.01-2007	International Society of Automation (ISA) "Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models," December 2007.
FIPS 140-2	Federal Information Processing Standards (FIPS) Publication 140-2, "Security Requirements for Cryptographic Modules," May 25, 2001.
Draft FIPS 140-3	FIPS Publication 140-3, "Security Requirements for Cryptographic Modules," to Supersede FIPS PUB 140-2, May 25, 2001, Draft issued July 13, 2007, still in draft status.
API 1164	American Petroleum Institute (API) STD 1164, "Pipeline SCADA Security," September 1, 2004. API 1164 is currently being updated by API and is going through internal review. The standard is estimated to be available for public use mid-year 2009.
CIDX	(This document was moved from Chemical Industry Data Exchange (CIDX) to the American Chemistry Council in 2006) "Guidance for Addressing Cyber Security in the Chemical Industry" Ver. 3.0, May 2006. This standard will be replaced by ISA 99, "Manufacturing and Control System Security, Part 2: Establishing a Manufacturing and Control System Security Program."
ISO 27001	International Standards Organization (ISO) Publication 27001:2005, "Information technology – Security techniques – Information security management systems – Requirements," First edition, October 15, 2005.
ISO 27002	ISO Publication 27002:2005, (replaced ISO 17799), "Information technology – Security techniques – Code of Practice for Information Security Management," renumbered 2007.
IEC 62351	The International Electrotechnical Commission (IEC) publication IEC/TS 62351, Parts 1-6, "Power systems management and associated information exchange—Data and communications security," May 15, 2007.
IEEE 1402	Institute of Electrical and Electronics Engineers (IEEE), Document IEEE 1402, "Guide for Electric Power Substation Physical and Electronic Security," January 30, 2000.
ISA 99.00.01-2007	ISA "ANSI/ ISA 99.00.01-2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models," October 29, 2007.
ISA 99.00.02-2007	ISA "ANSI/ ISA 99.00.02-2007, Security for Industrial Automation and Control Part 2: Establishing n Industrial Automation and Control System Security Program," October 29, 2007.
ISA 99.00.03-2007	ISA "ANSI/ ISA 99.00.03-2007, Security for Industrial Automation and Control Part 3: Operating an Industrial Automation and Control System Security Program," October 29, 2007.
ISA 99.02.01-2009	ISA "ANSI/ ISA 99.02.01-2009, Establishing an Industrial Automation and Control Systems Security Program," February 2009.
NERC CIP	North America Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, CIP-002 – CIP 009, standards on security topics, May 2, 2006.
NIST SP 800-40 R2	NIST SP 800-40, Rev 2, "Creating a Patch and Vulnerability Management Program,"
NIST SP 800-53	NIST SP 800-53, Rev. 3, Recommended Security Controls for Federal Information Systems – Information Security," July 2009.

f. *Catalog of Control Systems Security: Recommendations for Standards Developers*, January 2008, Appendix A, National Cyber Security Division, Control Systems Security Program, Department of Homeland Security.

Common Label	Description
NIST SP 800-61	NIST SP 800-61, Rev. 1, "Computer Security Incident Handling Guide," March 2008.
NIST SP 800-82	NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security, Final Public Draft 2009.
NIST SP 800-83	NIST SP 800-83, "Guide to Malware Incident Prevention and Handling," November 2005.
NIST SP 800-86	NIST SP 800-86, "Guide to Integrating Forensic Techniques into Incident Response," August 2006.
NIST SP 800-92	NIST SP 800-92, "Guide to Computer Security Log Management," September 2006.

The standards listed in Table 1 were selected for their relationship to control systems and represent a set of general cybersecurity guidelines that covers the widest range of sectors and standards applicable to ICS. An Internet search will reveal hundreds of additional guiding documents with publications coming from academic institutions, commercial firms, private consultants, and government agencies.

Automated tools are available to help an organization assess the secure posture of their ICS environment. They may be in the form of stand-alone software programs offered by commercial vendors or be products provided in conjunction with an assessment offered by a consulting firm. Also open source products could prove to be helpful.

A valuable self-assessment tool developed under the direction of DHS through the CSSP is the Cyber Security Evaluation Tool or CSET. This assessment tool is based on industry standards found in general IT and in specific ICS industry sectors. It assesses the security posture of a site based on answers to a series of questions that were developed based on the standards. CSET also provides a way to enter a diagram of the ICS with questions presented that correspond to each component in the diagram. The tool provides reports that indicate areas where a facility might improve and areas that should be addressed first. The splash screen for CSET is shown in Figure 4.

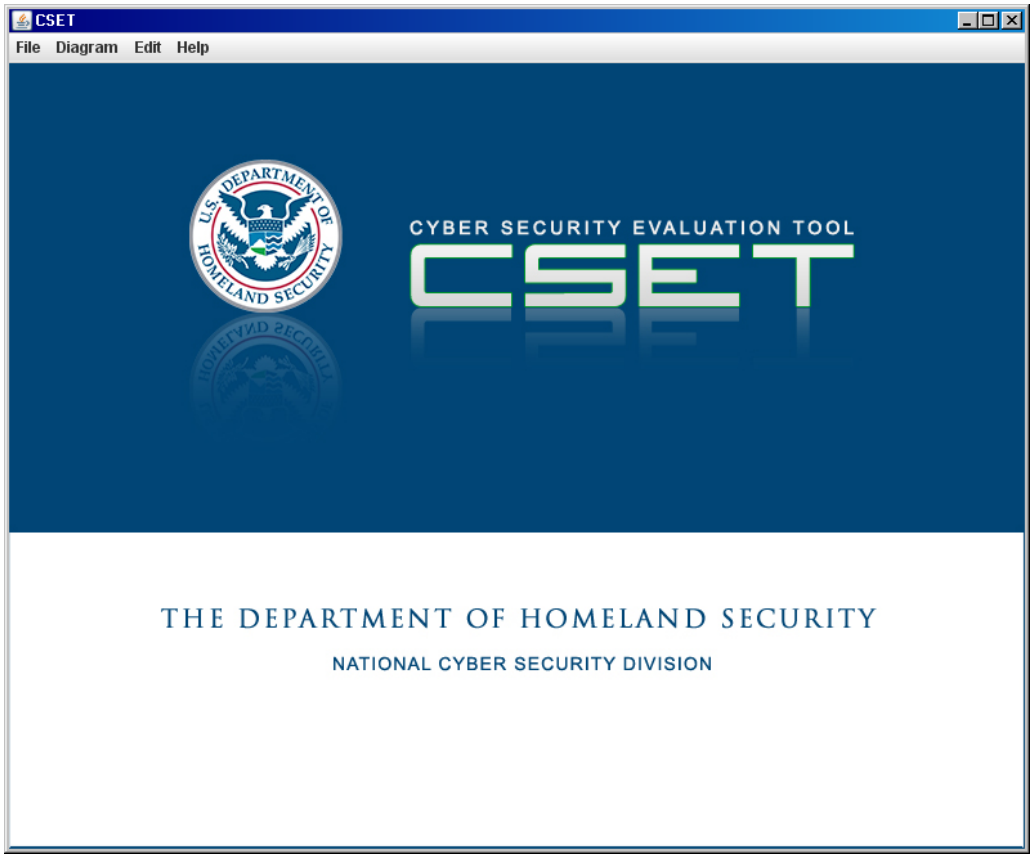

Figure 4. CSET opening screen.

3.2 Patch Management

Patch management is only one of many areas of consideration in an effective cybersecurity program. Patch management and vendor interaction are specifically highlighted in this document because of the unique requirements related to ICS. Patch management is important to incident response in two ways. First, and foremost, it is an essential means of preventing an incident from occurring. Second, patching is a way to respond to vulnerabilities and prevent reoccurrences of the exploit. Without patching, systems can be left in the same vulnerable state they were before the incident.

The following issues related to patch management[g] of ICS must be considered:

- Difficulties in scheduling maintenance windows on production systems to perform the patch
- Equipment that is no longer supported and no patches are available
- Patches that were issued by a third party—not the original vendor or supplier
- Testing of a patch in a nonproduction environment before implementing it on the production systems, especially where equipment is unique and expensive
- Creating a test bed or simulated environment

g. See the document: "Recommended Practice for Patch Management of Control Systems," DHS Control System Security Program (CSSP), December 2008.

- Creating a viable backup of the system configuration as a disaster recovery point of the working system, if the last known good configuration needs to be deployed
- Development of patch roll-back procedures, should it be discovered that a patch interferes with proper ICS operation
- Patches that cause issues with adjacent applications in the ICS
- Receiving patches from vendors in a timely fashion
- Accepting the testing processes used by the vendor, including both unit and integrated system tests
- Assuming the risk that the patch will not bring down or impact the production system
- Knowing the time it takes to deploy the patch, or knowing how long it takes to remove the patch if necessary
- Working with and patching software embedded in ICS components.

This paper does not discuss further details on patch management of control systems, but the document, "Recommended Practice for Patch Management of Control Systems,"[h] developed under the DHS CSSP program in December 2008 provides more detailed information on handling patch management of control systems. CSIRT staff is encouraged to review the patch management recommended practice as well as other guides to patching IT and ICS for general information and guidance.

3.3 Vendor Interaction

The need to work with vendors on cybersecurity is important in the ICS environment because of the proprietary nature of the software, the lack of maturity of the industry in relation to cybersecurity, and the more limited customer base of the vendors.

The business IT model has literally millions of users for a very limited number of operating systems, (or networking) vendors. This means that vulnerabilities in a single product like Linux or Windows, would impact nearly the entire customer base. Patching processes are more mature and well established, and vendor response is expected, even taken for granted. In addition, support for a single product or version of a product can be withdrawn with the expectation that the customer will upgrade to later versions. This is accepted practice in the IT environment and is often desirable so that new features are available to the customer base.

A single vendor is selling numerous products in the ICS model, and of those products, many versions are actively being used in the field. These products can have a long service life extending 20 years or more. In addition, the number of customers is relatively small when compared with products in the IT environment. In some cases, there may be only tens or hundreds of customers, depending on the product, its age, and how unique it is. With the pressure on vendors to support multiple products and versions of products, and with smaller numbers of customers demanding a fix, vendors cannot guarantee provisions for patches, state and status reporting, or fixes in a timely manner, if at all.

To ensure the highest degree of both prevention and response targeted interaction between the customer and the technical staff of the vendor are significant. A unified voice of all customers will be helpful in putting pressure on the vendor to address security issues with appropriate patches. Service level agreements must be established with vendors to ensure ongoing patches and related support. These agreements should not be allowed to lapse, or legal influence will be lost.

h. The document was developed to address issues specifically related to patch management of control systems. This is available on the US-CERT website.

Customers also can provide direction on priorities and customer needs. From the perspective of the product user, this would involve user groups and provide ongoing feedback to the vendor's technical and sales staff.

When responding to an incident, the relationship of technical or support staff at the vendor site is critical. Depending on the criticality of the ICS component, it might be necessary to include the vendor's technical personnel as an extension of the CSIRT or even part of it. This means that names, expertise, and contact information should be maintained. These people should know that they may be called on to assist in the event of an emergency. This arrangement may require contracts with service-level agreements that define what help can be expected and what the cost for that assistance would be. When an incident is happening, it is too late to be trying to set up new contracts with vendors. It is not practical in all cases, but advisable where possible, to include a turnaround time for patches or fixes in the agreement.

4. INCIDENT MANAGEMENT

This section discusses the four key parts related to managing a cybersecurity incident. Other documents related to incident response, which may expand or consolidate these primary activities, include: detection, containment, remediation, and recovery and restoration (see Figure 5).

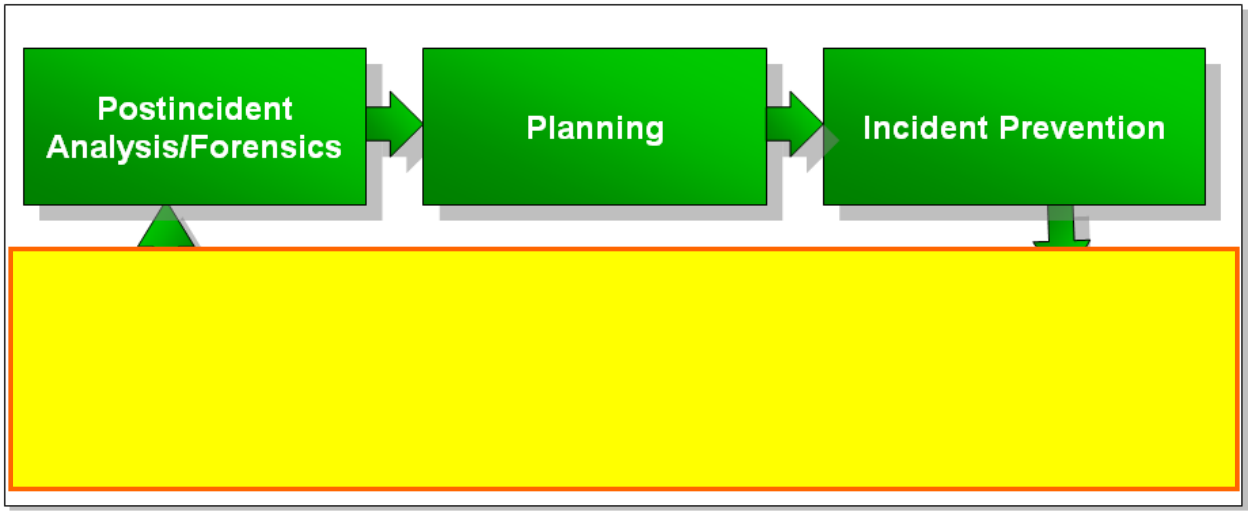

Figure 5. Managing an incident.

4.1 Incident Detection

Detecting an incident early will help to limit or even prevent possible damage to the ICS and reduce the downstream efforts to contain, eradicate, recover, and restore the affected systems. This section focuses on the methods of detecting cybersecurity incidents by discussing warning signs to indicate when a cybersecurity incident is pending, how to categorize and prioritize cybersecurity incidents and responses, and recommended detection steps. Assistance is also available through ICS-CERT if a suspected incident occurs, or help is needed with detection.

4.1.1 Reporting and Coordination

Working with ICS-CERT and other response organizations when an incident is suspected can enhance the team's ability to detect and understand the problem. Reporting both suspected and known incidents allows the experts at ICS-CERT[i] and other response organizations to understand and find solutions for the incident. A good chance exists that the situation being faced has happened before and information on detection, prevention, and recovery is immediately available. The staff supporting ICS-CERT can assist in all aspects of incident management if needed.

In addition to the ICS-CERT, other potential sources for coordination and information would include the Information Technology Information Sharing and Analysis Center (IT-ISAC) and other sector-specific ISACs including centers[j] for:

- Communications

[i] ICS-CERT is associated with the United States Computer Emergency Readiness Team (US-CERT). US-CERT is the operational arm of the National Cyber Security Division (NCSD) at DHS. To find more information, or to report an incident go to http://www.us-cert.gov.

[j] Information on the different ISACs can be found on the ISAC Council website at http://www.isaccouncil.org.

- Electricity Sector
- Emergency Management and Response
- Financial Services
- Highway
- Multi-State
- Public Transit
- Surface Transportation
- Supply Chain
- Water
- Research and Education
- Maritime and Research.

The mission statement of the IT-ISAC provides insight into the purposes and objectives of these organizations. As defined on their website, the mission of the IT-ISAC is to:

- "Report and exchange information concerning electronic incidents, threats, attacks, vulnerabilities, solutions and countermeasures, best security practices and other protective measures,
- Establish a mechanism for systematic and protected exchange and coordination of such information; and
- Provide thought leadership to policymakers on cyber security and information sharing issues."

Certain regulatory agencies such as the Nuclear Regulatory Commission may provide additional, sector specific information and may also require reporting of certain incidents.

4.1.2 Detection by Observation

Two general approaches can detect an ICS cybersecurity incident. The first is through user observation of abnormal system or component behavior. An observation can come from any member of the organization, including operators, process engineers, or system administrators. The second is through automated detection via applications or routines, such as network monitors, network traffic analysis applications, IDSs and antivirus programs that can detect and flag malware, intrusion attempts, policy violations, and exploits, as well as component failure. These automated approaches still require some human interaction for configuration, review, analysis, and action.

The approach requiring user observation is essentially an after-the-fact approach and can carry a number of adverse risks. After-the-fact means that an intrusion and cyber attack is currently taking place or has already occurred. Thus, this method provides no initial protection or prevention capability to a cyber incident. Some of the adverse effects associated with this approach are listed as follows:

- Damage to the physical system or equipment
- Extraction of critical control system operations data
- Alterations to the software configuration algorithms to produce future undesired system actions
- Injection of malware, such as viruses or worms, which compromises the confidentiality, integrity, and availability of the system or system data.

Every effort must be made to identify warning signs that could be observed prior to a system or equipment failure. Means other than a cyber attack can trigger many warning signs, but they are still worth considering as possible precursors to an incident. The following list of symptoms to be considered as possible indicators of an attack was taken from NIST SP 800-82, "Guide to Industrial Control Systems (ICS) Security (Final Public Draft)," September 2008, pp 6–19:

- Unusually heavy network traffic
- Out of disk space or significantly reduced free disk space
- Unusually high CPU usage
- Creation of new user accounts
- Attempted or actual use of administrator-level accounts
- Locked-out accounts
- Accounts in use when the user is not at work
- Cleared log files
- Full log files with an unusually large number of events
- Antivirus or IDS alerts
- Disabled antivirus software and other security controls
- Unexpected patch changes
- Machines or intelligent field devices connecting to outside Internet Protocol (IP) addresses
- Requests for information about the system (social engineering attempts)
- Unexpected changes in configuration settings
- Unexpected system shutdown.
- Other possible indicators of a cyber incident include:
- Stoppage or displayed error messages on a web, database, or application server
- Unusually slow access to hosts on the network
- Filenames containing unusual characters or new or unexpected files and directories
- Auditing configuration changes logged on the host records, especially disabling of auditing functionality
- A large number of bounced e-mails with suspicious content
- Unusual deviation from typical network traffic flows
- Erratic ICS equipment behavior, especially when more than one device exhibits the same behavior
- Any apparent override of safety, backup, or failover systems
- Equipment, servers, or network traffic that has bursts of temporary high usage when the operational process itself is steady and predictable.
- Unknown or unusual traffic from corporate or other network external to control systems network
- Unknown or unexpected firmware pulls or pushes.

The previous list provides examples of things to look for but is not exhaustive. It is recommended that a proper operational state be understood and documented if possible. Any deviation from the expected functionality could be considered a warning.

Operator experience may be the best source of detecting deviations from normal, because subtle differences in equipment behavior may create a "just doesn't feel right" situation that is difficult to identify. Very experienced operators will know when things are not working right and can detect potential cyber problems as well as non-security related equipment wear and tear.

Management should provide specific contact and reporting instructions to operators and any other plant personnel that may be in a position to detect unusual system or equipment behavior. This should include pager, phone, and e-mail information to allow the operator to contact the CSIRT. These instructions should also include a checklist of information to gather and report to assist the CSIRT in analyzing and accessing the unusual behavior. The contact information and checklist instructions should be posted in convenient and easily accessible locations.

4.1.3 Automated Detection Methods

Automated methods of incident detection can be extremely valuable in preventing exploits to the ICS. The nature of attacks, the number of attempts, and the round-the-clock timing of the attempts create an environment where manual observation is very difficult, if not impossible. Most networked ICS of any substance will have some type of automated detection capability. This may include sophisticated, commercial IDSs attached to the ICS networks or it may be simple firewall logging. It is essential that a proper balance of automation for the application be configured properly, be working as intended, and include the appropriate human review and interaction.

In Section 2.5 "System State and Status Reporting," describes different methods of automation. These include the various types of IDS such as NIDS, PIDS, and HIDS. Topics also discussed are vendor-developed or custom-built applications that reside on ICS components, which allow information to be gathered and reported.

The concept of system state and status reporting puts emphasis on using both commercial and customized methods to let the components of the system report on status and state information. This information is useful in preventing an incident, but is also valuable in post-incident analysis and forensics.

All automated detection systems have at least three components that are necessary for them to work properly:

- *A programmed method to detect an out-of-range or targeted event*. This may include the detection of a character string that matches a known virus signature or certain network behavior such as a denial-of-service attack. It also may detect attempts to access certain restricted ports, or it may recognize a known rogue IP source address. With individual ICS components, it could be a customized application that detects when the equipment or software behavior goes outside preset thresholds.
- *The ability to capture and report the event or change*. Detecting an event is the beginning; but to be of value, the application must organize and present the data in a useful format. More advanced systems will include filtering and reporting; others may just write log information to a text file. To be useful, specialized components must be able to write out or state changes in some form of audit or log file. Some processes cannot continuously be writing out a constant flow of log data without affecting equipment operations. In these cases, the ideal situation would be to set ranges and report only when outside the range.

- *Communication of flagged events to an operator*. Some sophisticated systems like an IPS may be able to take some preventative actions without human intervention. However, the IPS is designed for well understood IT applications and not for a production ICS where inadvertent shutdowns could have undesirable results. In a more typical situation, a human must be involved to decipher false-positives and to separate maintenance issues from potential cyber attacks. The human also must be able to respond to the data and initiate the appropriate response, including activating the CSIRT when necessary.

Each of the three components of an automated detection system must work properly or the system will fail. While the first two items have certain limitations, the major challenge seems to be with the practical aspects of the third—related to human observation and response. Some of the most significant challenges are related to availability, training in finding real events, and initiating a proper response when an actual event is discovered. The suggestions provided below address ways to support ICS personnel:

- Use centralized logging that consolidates a variety of data sources, allowing administrators to see a unified set of information presented in one place and in a consistent format. This may require interfaces to and data pulls from log files or audit tables.
- Develop necessary algorithms and business rules to filter and process raw log data (some IDSs already does some of this, this is referred to as log reduction). The objective is to simplify and automate the logic as much as possible so the operator does not have to constantly be reviewing raw data.
- Create effective communications capabilities between the automated, central program and the staff. This may include automated e-mail or page notification, and even audible alarms when necessary. The capability should be planned around both normal operations and times when experts may be gone, such as nights, weekends, and holidays.
- Set up an ongoing improvement program so that analysts are increasing their effectiveness in defining algorithms for detection, and operators are trained to better understand the data.

4.1.4 Incident Response Tools

In Section 2.5, different automated tools were mentioned to detect a potential incident during routine operations. Other tools are useful in capturing and analyzing more specific and detailed data. Some overlap exists as certain monitoring tools can be used for both ongoing monitoring and single incident detection and resolution. Incident response tool examples include:

- *Netflow Capture and Analysis*. These tools provide methods to capture and display the type of traffic crossing the network, including inbound and outbound traffic. These tools can isolate data by applications, conversations, domains, endpoints, and protocols. Many of these tools will also store data for both analysis and forensic work.
- *Network Performance Monitors*. They provide additional insight into network performance and can help identify where out-of-normal performance is occurring. They may also include bandwidth monitoring and analysis as well as network routing analysis.
- *Availability Monitors*. These tools can assist in determining if network devices are available with advanced “ping” capabilities such as displays of real-time response rates.
- *Application Monitors*. A specific application can be monitored if there is suspicion of unauthorized access or manipulation. These tools allow a more granular analysis of a suspected application as compared with overall network monitoring.

- *Packet and Traffic Reconstructors.* Often associated with, or bundled as part of a network traffic monitor, these tools reconstruct files back into their original format on the network, capturing a static image of the network and the associated traffic.
- *Protocol Analyzer*. Similar to other tools mentioned above, this tool/feature captures and stores for potential forensic analysis packet information, including consolidated statistical information.
- *Trace Route and Whois tools*. These can be helpful in tracing an intruder to the location of the source computer. Associated functions allow IP address blocking and reporting.

4.1.5 Incident Categorization

Once positively identified, a cyber attack should be categorized, and the response prioritized based on that categorization. The categorization should be based on the type of incident and the potential damage to the ICS. The type of incident will drive the appropriate level of response. The incident response plan should outline in detail what the level of response (and level of effort) should be for each type of incident. As mentioned earlier, this planning should occur well in advance of an actual event.

The prioritization of the response should be based on the current and potential effect to the ICS, and the criticality of the effected equipment and system to company operations.

The following questions will aid in determining the categorization/prioritization criteria:

- How did the exploit occur and can it happen again? In what timeframe?
- Was this internal or external to the organization?
- What type of attacker tools were placed onto the system, if any?
- What networks and systems are affected by the attack vector, and can the problem spread to other sites and customers?
- Are there legal or safety issues caused by the attack?
- How much does the impact increase if the incident is not contained within hours or days?
- Can systems safely fail-over or continue operating?
- How important are the effected components to the ICS and to operations in general?

The following are recommended categorization/prioritization steps to take:

1. Assign a principal investigator responsible for identifying and mitigating each incident.
2. Validate if the incident is a malicious or non-malicious occurrence. If the event is non-malicious, the full CSIRT will not be required, though some resources may be used to solve the problem.
3. Identify and evaluate the evidence in detail and keep accurate documentation with controlled access to the evidence.
4. Coordinate with the specific personnel that provide operating business unit network services to the effected system.

Specific steps unique to the organization should be included. They should be clearly defined in the incident response plan and should guide the actions of the CSIRT when categorizing and prioritizing an incident.

4.2 Containment

While containment often focuses on preventing the spread and effects of malware, several other types of incidents will require other actions related to containment. An example would be an employee who accesses unauthorized information by using another person's user account and password. Containing the situation would require removing the employee from access to the information and then enforcing disciplinary action as necessary. For an attacker who did not leave malware on the system, but was directly accessing ICS components, containment would include blocking the intruder, restoring the equipment, if affected, and then applying protective steps as outlined in Section 3 on Prevention.

The primary case for containment is where malware in some form has been left on the ICS. This section will focus on containment issues related to software that has been placed on servers or other components that will either create an access path for an intruder, or will independently run to cause harm to the ICS. Additional information can be found in NIST SP 800-83, "Guide to Malware Incident Prevention and Handling," issued in November 2005.

There are two main purposes in the containment of malware. The first purpose is to stop the spread to other parts of the system. The second purpose is to prevent continued damage to the ICS. Even if the malware is isolated from spreading to other components or networks in the ICS or across facilities, it may and can continue to cause damage in the isolated segment.

The containment of malware does not follow a standard approach for each organization. It will vary based on the type of malware, the importance of the effected system, and the acceptable level of risk. Thus, every organization must determine its proper containment actions based on its unique system requirements. The containment criteria need to be well documented and understood by members of the organization and the CSIRT.

Several methods to malware containment are available. The first method uses automated technologies such as virus removal programs to eliminate the problem and restore system functions. The second method halts services while the incident is being handled, and the third method blocks certain types of network connectivity by using a filtering process.

Using automated technologies provides immediate detection and response if the user chooses to program the application in this manner. This method can only act against known malware and cannot remediate Zero Day vulnerabilities. Zero Day exploits target vulnerabilities for which there is no available patch. These tools can significantly reduce cyber threats by acting as a filtering process or first defense, which can save organization resources and reduce system downtime. One of the challenges to the control system engineer is finding automated applications that handle unique ICS components, especially those that are using dated or unique protocols.

Temporarily halting services is a more drastic and potentially disruptive measure typically executed at the application level such as disabling a service. This could occur on a server or at the network level such as using firewalls to block IP addresses or ports associated with a service. Halting specific affected services stops and prevents the rapid spread of the infection while maintaining operation of the unaffected components to avoid complete loss of service. The desired goal is to contain the incident effectively with the least amount of loss in functionality. To effectively prepare for halting services, an organization must maintain a list of network and component services used along with their associated Transmission Control Protocol and User Datagram Protocol ports.

Using containment through disabling connectivity is an effective and quick means of temporarily restricting network connectivity to infected systems attempting to establish connection to an external system. This can prevent malware from downloading and prevent the spread of that system's infection to other internal networked systems. The intention is to isolate the critical control system from the network

by removing the networking communication point and then to test and verify isolation without disrupting other critical services. This method of disconnecting critical ICS network components should be identified and tested in the incident planning and preparation stage[k].

4.3 Remediation

Prior to full system recovery, remediation efforts should be performed to fix the source of the problem. This may include eradication of any malware left on the system, removal or replacement of vulnerable equipment, reconfiguration and patching of equipment or software, and possible access cancellation for certain personnel.

If the incident involved unauthorized access then efforts should be made to close the access path. This may include changing all passwords and certain user names. Efforts may also include blocking access from identified IP addresses and changing of port configurations on firewalls.

Careful analysis should be performed on the ICS to verify the path taken by the intruder. This should not only expose the actual weakness, but it can also highlight similar areas that may need attention. A specific dial-up device may have been the culprit, but other comparable devices may be scattered throughout the ICS that are just as vulnerable.

If the incident involved malware left on the system, then removal or eradication will be necessary. Ideally, eradication will remove the malware with the least amount of disruption to the facility's operations. This process of removing malware could take some time to successfully accomplish, depending on the type of malware, severity of the infection, and containment method used.

Many techniques can remove malware from an infected system. The most common method is using automated eradication tools such as antivirus software, spyware detection and removal utilities, and patch management software. Other options include restoring a system to a set point before the infection or reloading key system files. These tools can quickly find and remove malware if they have detected the infection. Unfortunately, most antivirus type programs focus on typical IT systems and would not detect malware on more specialized control systems. There is also the danger that these utilities will remove or alter legitimate system or data files. In these situations, manual removal may be necessary with help from the vendor, or the vendors themselves may be able to provide removal software that has been tested against the target system.

For more severe cases of malware infection, a rebuild may be required. This technique would encompass reinstallation and securing of the operating system and application followed by restoring data from backup files.

A complete rebuild should be considered if the following system characteristics are present:

- The intruder gained root or administrator-level access to the system.
- Back-door type access has been granted that is not readily identified. The risk is that one back door may be found, but others may go undiscovered.
- System files were replaced by the malware or directly by the intruder.
- The system is unstable or does not function properly after antivirus software, spyware detection and removal utilities, or other programs or techniques eradicate the malware. This indicates that either the malware has not been eradicated completely or that it has caused damage to important system or application files or settings.

[k] Halting services can have a significant impact on operations. CSSP recommends that these actions be taken with extreme caution and only after extensive testing on nonproduction systems.

When the eradication efforts are finished, it is highly recommended that testing be conducted to verify that the ICS is working as intended. This includes not just observable behavior, but also reviewing any incident detection information to look for underlying signs of remaining rogue code.[1]

4.4 Recovery and Restoration

The ICS environment introduces additional complexities related to recovery and restoration that would not be found in typical IT systems. However, some commonalities with traditional IT include removal of malware, restoring backup data to databases, systematically removing temporary containment actions, and restarting all operational systems and applications.

The additional complexities in the ICS are related to the manner in which systems must be managed as part of the incident response. Because many of the services provided by the facility cannot be shut down during the response, other approaches have to be taken. These include switching the control functions to fail-over systems, moving to backup equipment that is temporary or has limited capabilities, or isolating system components from network access. In these situations, the vital equipment and processes continue to operate, but in a temporary state with limited integration and, in some cases, reduced functionality.

Because of the demand for continuous operation, this temporary operational state is has a higher risk for the enterprise. Having redundant systems in place is expected in most critical situations but, triple redundancy, while ideal, is not always possible due to high costs and architectural complexities. As a result, if the backup systems fail, production stops, which puts great pressure on the CSIRT and operational staff to restore operations as soon as possible.

Information on restoring traditional IT components can be found in computer security documents, such as NIST SP 800-61, "Computer Security Incident Handling Guide," issued in January 2004 and other sources mentioned in the recommended reading at the end of this document. Specific recommendations for ICS follow:

- Establish contingency plans with available equipment (even portable equipment if necessary) identified before the incident. This will allow operations to continue while primary systems are being restored.
- Patch and maintain all backup systems to the same level as the primary systems.
- Conduct regular and planned testing at a planned specific time to verify that the fail-over systems will work properly when called upon.
- Establish plans to run segments of the ICS in isolation prior to an incident. This will provide the engineers a realistic picture of interdependencies between components, allowing them to make decisions on isolation, if necessary.
- Test backup equipment against realistic timeframes found in a worst-case scenario. For example, backup generators may need to power a system for days rather than hours, depending on the circumstances of the facility.
- Establish and run acceptance tests and procedures to ensure that systems have been restored to the pre-incident state. These may include both automated and manual tests.
- Define procedures as part of the incident response plan to provide for the proper authority to accept the tests and declare the ICS fully operational.

[1] In all cases where basic system files are being modified or removed, the CSSP highly recommends extensive testing of tools and procedures prior to changes to the production systems.

As discussed in Section 5, the final stage of recovery is to not just restore the system to where it was, but rather to make it better and more secure. The system should have the same operational capabilities, but it also should protect against the exploit that caused the incident in the first place.

5. POSTINCIDENT ANALYSIS AND FORENSICS

Post-incident analysis and forensics consists of three subject areas. The first area is lessons learned where an attempt is made to analyze the incident, the response, and the impact to discover and document what could have been done differently to improve the response. The second area is recurrence prevention, or actually applying what was learned in remediating discovered weaknesses in the cybersecurity program, including preventing a similar incident. The third area is forensics, which includes capturing and protecting data as evidence for potential legal action.

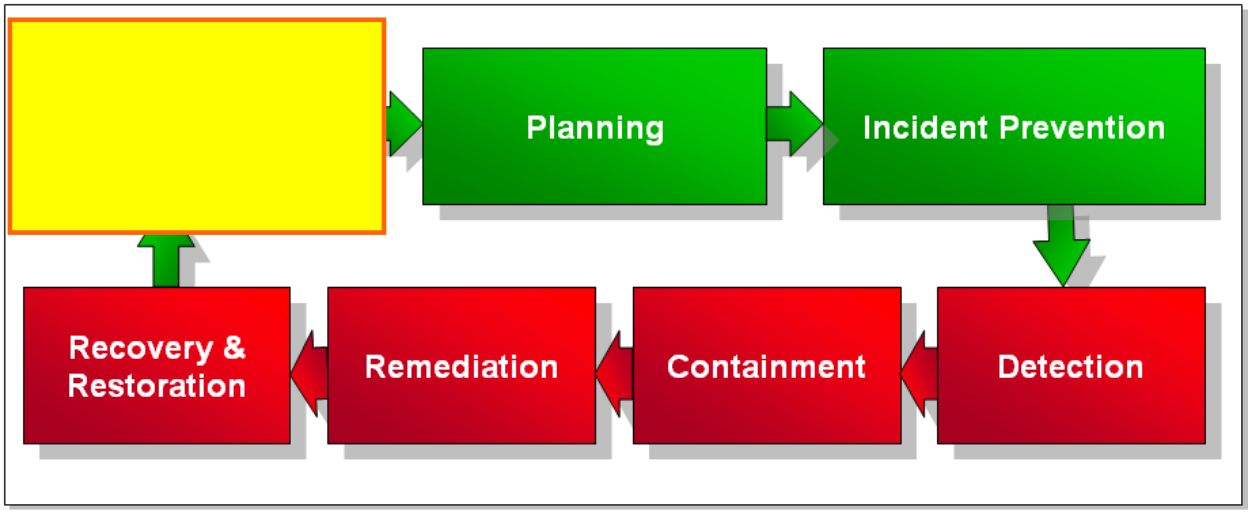

Figure 6. Post-incident analysis and forensics.

5.1 Lessons Learned

Unfortunately, cyber attacks are dynamic, with attackers learning quickly from their successes and capitalizing on failed or incomplete defenses. Every cyber event provides an opportunity to see clearly the weaknesses in the security posture of the control systems. It also reveals any weaknesses in the way the organization handles its response. Performing a lessons learned exercise is essential to identifying weaknesses and preventing the reoccurrence of mistakes.

Any incident, whether successful or not, should be used as a chance to gain additional information to secure the ICS. For example, a near hit, where an outside reconnaissance effort is detected yet not exploited, can provide valuable information. Much useful data can be discovered by extensive review of the logging functions of firewalls, routers, switches, servers, and workstations. This allows the analyst to determine a baseline of normal activity and how unauthorized access is attempted or successfully completed. An incident need not be limited to only a physical attack on a system. Other attempts to gain access include non-cyber related activities such as social engineering or email phishing attempts to get recipients to reveal data, passwords, or account configuration information.

A lessons learned exercise should be performed after every identified incident. Doing so will allow the incident to be reviewed so that access paths in system security can be identified and closed. If the problem is not found and fixed, the attack can be repeated, only with greater ease and frequency.

It is highly recommended that other incidents, beyond those of the facility, be considered for review. This is an ideal opportunity to continuously improve the security posture of the ICS without having to suffer the damages of an actual incident. Because most organizations are not anxious to publish the details of a security incident, it will be necessary to work closely with CSSP and ICS-CERT, and other CSIRTs to identify incident information and any lessons learned from the affected organization. Because a large organization may have several similar facilities, it is essential that lessons learned information be shared across all internal sites.

A lesson learned exercise should be held as soon after the incident as possible. This will typically follow the recovery and restoration phase. Any delay in conducting this exercise will leave the ICS vulnerable to additional, similar exploits. Guidelines for conducting this exercise are as follows:

- All members of the internal CSIRT should participate if at all possible; the different perspectives and experience base will produce valuable perspectives.
- The CSIRT Team Manager should assume responsibility to call and organize the lessons learned exercise. Notes should be taken of both the discussion and the action items.
- Information should be sought from external sources, including vendors, integrators and other national and subject-specific incident response teams such as ICS-CERT. This will provide additional details on the exploit and ways that others have mitigated the vulnerability.
- Key questions should be answered, including:
    - What components were affected—type, manufacturer, etc.?
    - What operating systems, including embedded ones, were affected?
    - How access was gained?
    - What damage was done and what potential damage could have been done?
    - What network vulnerabilities, if any, allowed access to the ICS?
    - What standards and technical solutions might have prevented the incident?
    - What procedures and policies might have prevented the incident?
    - What training is necessary to prevent additional exploits?
    - How was the incident detected, and could it have been found earlier or prevented?
    - Are we still vulnerable and for how long?
    - Have vendors provided any patches or other solutions, and if so, were they implemented in the ICS in a timely manner?
    - What were the breakdowns in the incident response, including equipment, communications, lines of authority, vendor interactions, analysis, decision-making, and recovery?
    - What areas need to be improved and have processes changed?
    - Can this information be shared with trusted partners?
    - Can this information be shared with appropriate government agencies, including response teams?
- Based on the identification of weaknesses, specific assignments should be given to participants to systematically address each concern. The CSIRT Team Manager should take responsibility to see that all actions are completed in a timely manner to prevent additional exploits.

5.2 Recurrence Prevention

Once a vulnerability has been discovered, it will remain an open door until preventive action is taken. One of the primary purposes of the lessons learned exercise is to analyze the incident and initiate action to

prevent a recurrence of the exploit. A review of overall incident prevention would be helpful (See Section 3, “Incident Prevention”).

In addition to the suggestions made in Section 3, a facility also might do one or more of the following on the incident:

- *Identify access methods*. Identifying access methods may be simple or difficult, depending on the incident. An incident that was caused by an employee or contractor with inside access would be easy to identify but difficult to resolve because legitimate access must be provided. Preventive actions may include increased background checks, better training, and access control based on a stronger need to know and role responsibility in the organization. Other incidents may involve malware that was loaded on a server. The solution might include removal of the malware followed by additional antivirus support and more detailed user training on social engineering and prevention techniques. A more difficult situation, where the access method is hard to discover, might include a skilled intruder that erased network logs, spoofed timestamps, or used compromised accounts that had necessary or administrative access to the ICS. If the method cannot be discovered by the internal CSIRT, it may be necessary to call in expert help to discover the method. If the access path cannot be found, then, as a last resort, the facility should conduct a systematic effort to strengthen all possible access paths.
- *Understand intruder motivation*. Because it would be difficult to assign resources to every aspect of the ICS, it is practical to increase security in specific targeted areas. For example, if the motive is to steal information, then databases would most likely be the target and securing key database servers and management systems would be the immediate priority. If public chaos, harm, and publicity are the desired outcomes, certain ICS components may need attention. If the motive is financial damage to the company, production processes might be targeted. Understanding the motives allows more immediate and focused attention on specific aspects of the ICS environment.
- *Assess and strengthen specific ICS components*. Access methods typically involve the network, but the incident might expose vulnerabilities related to specific models or types of components. This assessment can expose un-patched components, outdated equipment, or open communications between components. Solutions include equipment replacement, patching, and strengthening boundaries around components in the ICS where components cannot be easily replaced. This analysis may provide cost justification for replacement of dated system components.
- *Review detection methods*. When an incident occurs in a facility, the detection methods typically were not strong enough to identify the attempt in the early stages. For example, reconnaissance activities may have been going on for days or weeks before the actual exploit. Solutions might include stronger intrusion detection methods and software applications or a greater need for log reviews and analysis.

5.3 Forensics and Legal Issues

Computer forensics is most commonly associated with the collection and preservation of information and evidence for use in legal actions against the person or organization that caused the incident. However, in the context of this recommended practice it is much more than just gathering information to help understand and analyze the incident. The lessons learned exercise identifies and analyzes vulnerabilities leading to ways of protecting the ICS against future attacks, which focuses on gathering information like formal cyber forensics, but does not have the very stringent requirement of preserving and protecting the data that are found. Informal forensics as defined here also ignores requirements for the handling of evidence that would be found in the formal processes. The objective of informal data gathering and analysis is, therefore, to strengthen the ICS. The objective of formal forensics is to collect acceptable legal evidence to support criminal proceedings.

Complications can occur for both informal and formal forensic activities. For example, many RTOS in control system components use memory while running. Corrupted kernels are erased when the power is removed, and upon power restoration, the basic kernel is reloaded with its original set point parameters. If the kernel was modified during a cyber attack, currently no easy method is available to log and preserve the state of the RTOS kernel at the time of attack. It may be possible to take a snapshot of the kernel on the isolated component for later analysis under two conditions: the offending component is isolated by disconnecting it from the network, and leaving it in a powered state.

In most incident instances, the system administrator or process engineer's priority is to resume normal operations as soon as possible, often by rebooting the affected device. When this process is executed in this manner, evidence may be destroyed. If this action is necessary, other forensic means to gain information may be available. Some of these means are server system logs, firewall entry and exit logs, and switch logs. These options may not be available due to poor configuration or inability of devices to preserve these artifacts.

On the opposite extreme, if too much data were to be logged this could overwrite or destroy useful information. This is true for most IT elements. Several major impediments to activation of logging also include housekeeping chores such as reviewing logs for unusual or abnormal activity, purging old logs, archiving, and preserving specific logs. If done correctly, these logs are indispensible in determining what activity happened, when it happened, and how it happened. But if done incorrectly, logging generates a large amount of data and activity with limited value added to the forensics investigation.

This document will not expand further upon the details of forensics in ICS. Another recommended practice, also developed under the CSSP should be consulted for details on both formal and informal forensics and data gathering in control systems. The document is "Recommended Practice: Creating Cyber Forensics Plans for Control Systems," August 2008, DHS Control Systems Security Program.

Several guidance documents; such as NIST SP 800-61 "Computer Security Incident Handling Guide," NIST SP 800-86 "Guide to Integrating Forensic Techniques into Incident Response," and the CSSP's "Creating Cyber Forensics Plans for Control Systems"; provide additional reference information for forensics in ICS.

6. CONCLUSION

The steps described in this paper provide ICS users the basis to establish an incident response capability that includes analysis and understanding of the ICS environment, preventative actions, and ways to respond to and manage an incident should it happen.

Three sets of actions are emphasized:

- Learn from the experiences of previous incidents, both internal and external to the organization
- Prepare for an incident with an effective response plan with well thought out policies and procedures
- Assess the vulnerabilities within the ICS and then implement protective measures to safeguard those systems.

For situations when a cyber incident does take place, additional reactive actions are discussed. They include ways to detect an incident, contain the effects of it, remove the threat from the ICS, and restore the system to normal operations.

With an increasing threat from more sophisticated and motivated parties, and with the ever growing integration of ICS into corporate networks, and even the Internet, the tenants presented in this and other incident response documents should be incorporated into the plans and procedures of critical facilities. Doing so will prevent many issues from arising and will allow the facility to respond, if necessary, in a successful and effective manner.

6.1 Recommended Reading References

"Guide to Industrial Control Systems (ICS) Security," National Institute of Standards and Technology (NIST) Special Publication 800-82 (Final Public Draft), September 2008, Keith Stouffer, Joe Falco, Karen Scarfone.

"Computer Security Incident Handling Guide," NIST Special Publication 800-61, January 2004, Tim Grance, Karen Kent, Brian Kim.

"Guide to Malware Incident Prevention and Handling," NIST Special Publication 800-83, November 2005, Peter Mell, Karen Kent, Joseph Nusbaum.

Handbook for Computer Security Incident Response Teams (CSIRTs), Carnegie Mellon Software Engineering Institute, 2nd Edition, April 2003, Moira J. West-Brown, Don Stikvoort, Laus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek.

"Recommended Security Controls for Federal Information Systems," NIST Special Publication 800-53, Rev. 2, December 2007, Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, George Rogers.

Security Guidelines for the Petroleum Industry, Third Edition, April 2005, copyright 2005, American Petroleum Institute.

Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, October 2004, American Petroleum Institute.

"Recommended Practice for Patch Management of Control Systems," DHS Control System Security Program (CSSP), December 2008.

"Technical Article: Security Incidents and Trends in SCADA and Process Industries," May 2007, Eric Byres, David Leversage, and Nate Kube.

Guidance Document "Guidance for Addressing Cyber Security in the Chemical Industry," American Chemical Council and ChemITC, Version 3.0, May 2006.

"Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," July 2002, Computer Crime and Intellectual Property Section – Criminal Division – United States Department of Justice.

"Creating Cyber Forensics Plans for Control Systems," DHS Control System Security Program (CSSP) August 2008.

6.2 Websites

http://www.kb.cert.org/vuls/

http://csrp.inl.gov/Documents/Forensics_RP.pdf

http://www.cpni.gov.uk/Docs/Guide_3_Establish_Response_Capabilities.pdf

http://www.cpni.gov.uk/

http://www.cpni.gov.uk/Products/bestpractice/3692.aspx

http://www.doecirc.energy.gov/index.html

http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf —Creating a Patch and Vulnerability Management Program

http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf —Information Security

http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf —Computer Security Incident Handling Guide

http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf —Guide to Malware Incident Prevention

http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf —Guide to Integrating Forensic Techniques into Incident Response

http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf —Guide to Computer Security Log Management

http://www.americanchemistry.com/s_chemitc/sec.asp?CID=1641&DID=6201

http://www.first.org/

http://www.enisa.europa.eu/cert_guide/pages/01.htm

http://nvd.nist.gov/home.cfm

http://www.isa.org/

http://www.americanchemistry.com/s_acc/index.asp

http://www.americanchemistry.com/s_chemITC/

http://www.usdoj.gov/criminal/cybercrime/

http://www.us-cert.gov/control_systems/csdocuments.html

7. GLOSSARY

Computer Emergency Response Team Coordination Center (CERT/CC). The CERT/CC was started December 1988 by the Defense Advanced Research Projects Agency, which is part of the U.S. Department of Defense. The purpose of CERT/CC was to study Internet security vulnerabilities, provide services to websites that have been attacked, and publish security alerts. CERT/CC now resides at the Software Engineering Institute operated by Carnegie Mellon University.

National Infrastructure Advisory Council (NIAC). NIAC provides the President of the United States through the Secretary of Homeland Security with advice on security of critical infrastructures, both physical and cyber, supporting the 18 sectors of the economy. It has the authority to provide advice directly to the heads of other agencies such as Health and Human Services, Transportation, and Energy. NIAC is charged to improve the cooperation and partnership between the public and private sectors in securing critical infrastructures, and advises on polices and strategies ranging from risk assessment, information management, information sharing, protective strategies, and clarification of roles and responsibilities between public and private sectors.

National Vulnerability Database (NVD) Version 2.2. The U.S. Government's repository of standards based on vulnerability management data represented using the Security Content Automation Protocol. This database consists of databases of security checklists, security-related software flaws, misconfigurations, product names, and impact metrics. NVD supports the Information Security Automation Program.