Bellingham, Washington, Control System Cyber Security Case Study[1]

Marshall Abrams, The MITRE Corporation, abrams@mitre.org
Joe Weiss, Applied Control Solutions, joe.weiss@realtimeacs.com

Abstract

Cyber security often focuses on the vulnerabilities of commercial off-the-shelf software and Internet access, with the primary concern being malicious activity. There have been fewer discussions about control system cyber security and how control system cyber security policies and countermeasures can potentially preclude, or minimize, the impacts of a control system cyber security event. This paper examines an actual control system cyber security event that resulted in significant environmental and economic damage as well as deaths. In this case, operating policies and procedures had readily identifiable cyber security vulnerabilities. The paper examines the timelines, control system response, and control system policies that were in effect at the time of the event. The paper then identifies the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems*, management, operational, and technical safeguards or countermeasures that, if implemented, could have prevented the event.

Overview

On June 10, 1999, a pipeline owned by Olympic Pipeline Company ruptured and gasoline leaked into two creeks in Bellingham, Washington. The gasoline ignited, resulting in a fireball that killed three persons, injured eight other persons, caused significant property damage, and released approximately ¼ million gallons of gasoline, causing substantial environmental damage.

The pipeline system is remotely operated from a central control center where pipeline controllers can monitor key variables, monitor, and operate mechanical components, such as pumps and motor-operated valves. The pipe rupture involved a complicated scenario of physical damage to the pipeline, with an eventual pressure buildup not mitigated by the pipeline Supervisory Control and Data Acquisition (SCADA) system or identified in a timely manner by the leak detection systems.

A number of events and conditions set the stage for the pipeline rupture:

- External damage to the pipeline in the vicinity of the eventual rupture caused by a contractor installing water lines across the pipeline.
- During construction of the Bayview products terminal, pressure relief valves were installed that were found to be improperly configured or adjusted, and the actions taken by the company to test and correct the valve settings were ineffective.

1 This work was performed under NIST contract in support of the Industrial Control System Security Project.

- On the day of the accident, the SCADA system that controllers used to operate the pipeline became unresponsive.
- At the time of the accident, the system administrator may have been programming some new reports on a terminal in the control center computer room. This factor is open to question because key personnel have refused to respond to questions, exercising their Fifth Amendment rights, and the records entered just before the unresponsiveness were deleted to stop the abnormal computer operations.

This case study examines the event from a cyber security perspective. It provides the detailed timelines and discusses the associated cyber issues, examines the NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, controls that were violated or not met resulting in the degraded SCADA performance, and posits the potential mitigation that would have occurred if the SP 800-53 controls had been followed. Applicable controls and control families are:

- Policy and Procedures
- Access Control
- Audit and Accountability
- Awareness and Training
- Certification, Accreditation, and Security Assessments
- Configuration Management
- Contingency Planning
- Incident Response
- Media Protection
- System and Communications Protection
- System and Information Integrity

Table of Contents

Introduction

This case study is intended to help engineers and managers implement an ongoing Industrial Control System (ICS) cyber security program by providing an example of an actual control system cyber security event that resulted in three deaths as well as significant environmental and economic damage. In this case, operating policies and procedures had readily identifiable cyber security vulnerabilities. The case study examines the timelines, control system response and control system policies that were in effect at the time of the event and identifies management, operational, and technical safeguards or countermeasures that, if implemented, could have mitigated the event. This case study complements NIST Special Publication 800-82 *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*[2]

Figure 1. Gasoline Fire

On June 10, 1999, at about 3:30 p.m. Pacific Daylight Time (PDT), a 16-inch diameter pipeline owned by Olympic Pipeline Company ruptured, and gasoline leaked into the Hanna and Whatcom Creeks in Whatcom Falls Park within Bellingham, Washington (see Figure 1). At about 5:02 p.m., the gasoline ignited, resulting in a fireball that traveled approximately 1 1/2 miles downstream from the pipeline failure location. Two 10-year-old boys and an 18-year-old young man lost their lives as a result of this tragic accident. Eight additional injuries were documented, along with significant property damage to a single-family residence and to Bellingham's water treatment plant. The release of approximately ¼ million gallons of gasoline caused substantial environmental damage to the waterways.[3]

2 **NIST Special Publication 800-82** *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security*, initial public draft, September 2006. http://csrc.nist.gov/publications/drafts.html#sp800-82

3 Testimony of Robert Chipkevich, Director Office of Pipeline and Hazardous Materials Safety National Transportation Safety Board before the Committee on Commerce, Science and Transportation United States Senate

This case study analyzes the event to determine how the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53[4] controls might have prevented or mitigated the event. NIST is now augmenting SP 800-53 by adding interpretations and guidance for ICSs[5]. This case study incorporates those extensions.

The Bellingham event has been documented in a National Transportation Safety Board (NTSB) report[6] and other documentation available in the public domain. The pipeline system is remotely operated from a central control center where pipeline controllers can monitor key variables, such as pressures and flow rates, and can also monitor and operate mechanical components, such as pumps and motor-operated valves. The pipe rupture involved a complicated scenario of physical damage to the pipeline with an eventual pressure buildup not mitigated by the pipeline SCADA or leak detection indication in a timely manner. The case study examines the event from a cyber security perspective. It provides the detailed timelines and cyber issues, examines the NIST SP 800-53 controls that were violated or not met resulting in the degraded SCADA performance, and posits the potential mitigation that would have occurred if the NIST SP 800-53 controls had been followed.

Structure of this Case Study

A brief discussion of Cyber Security in ICSs and SP 800-53 and related documents follows the overview and introduction. A system description introduces the Bellingham incident. The incident description includes SCADA system performance; timeline; investigation, analysis, and observations; relevant National Transportation Safety Board (NTSB) accident board findings, probably causes, cyber security issues in the incident, and recommendations. NIST SP 800-53 controls that might have prevented or ameliorated the impact are discussed; -policy and procedures;, access control; audit and accountability; awareness and training; certification, accreditation, and security assessments; configuration management; contingency planning; incident response; media protection; system and communication protection; and system and information integrity. The NIST minimum security control baselines are presented in an appendix.

Cyber Security in Industrial Control Systems

ICS encompasses several types of control systems, including SCADA systems, Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), and other smaller control system configurations often found in the industrial control sectors. Many ICSs in use today were developed years ago, long before public and private networks,

---

Regarding the Bellingham, Washington, Pipeline Accident March 13, 2000. http://commerce.senate.gov/hearings/0313chi.pdf

4 *Recommended Security Controls for Federal Information Systems,* National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, December 2006, http://csrc.nist.gov/publications/nistpubs/800-53-Rev1/800-53-rev1-final-clean-sz.pdf

5 *Draft ICS Augmentation of SP 800-53,* May and June 2007. http://csrc.nist.gov/sec-cert/ics/draft-ics-interpretation_SP800-53.html

6 *Pipeline Accident Report, Pipeline Rupture and Subsequent Fire in Bellingham, Washington June 10, 1999,* NTSB/PAR-02/02, PB2002-916502. http://www.ntsb.gov/publictn/2002/PAR0202.pdf,

desktop computing, or the Internet were common parts of business operations. The need for information security measures within these systems was not anticipated, and at the time, security for ICSs meant physically securing access to the network and the devices that controlled the systems. As Information Technology (IT), including microprocessor, personal computer, and networking, evolved during the 1980s and 1990s, ICS design changed to incorporate modern information technologies, such as the use of commercial off-the-shelf-products (e.g., Microsoft Windows operating systems) and open protocols (e.g., Transmission Control Protocol/Internet Protocol). Internet-based technologies started making their way into ICS designs in the late 1990s. These changes to ICSs exposed them to new types of threats and significantly increased the likelihood that they could be attacked or inadvertently affected.

NIST Special Publication 800-53 and Related Documents

NIST has established an Industrial Control System Security Project[7] to improve the security of public and private sector ICS. NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, provides implementing guidance and detail in the context of two mandatory Federal Information Processing Standard Publications (FIPS PUBS) that apply to all federal information and information systems, including ICSs. FIPS 200 *Minimum Security Requirements for Federal Information and Information Systems* requires that federal agencies implement minimum security controls for their organizational information systems based on the FIPS 199 *Standards for Security Categorization of Federal Information and Information Systems* security categorization of those systems. Private sector and other organizations may consider the use of these standards and guidelines as appropriate. NIST is working with all stakeholders and other interested parties to develop convergent guidance on the application of these security requirements for ICS.

The NIST ICS Security Project is augmenting SP 800-53 to address ICS. SP 800-53, which was developed for traditional information systems, contains a security control catalog (Appendix F) and mandatory information security requirements for all non-national security information and information systems that are owned, operated, or controlled by federal agencies (Appendices D and E). While most controls in SP 800-53, Appendix F, apply to ICS as written, several controls require ICS-specific augmentation by adding one or more of the following:

- ICS Supplemental Guidance
- ICS Enhancements (one or more)
- ICS Enhancement Supplemental Guidance

When augmenting Appendix F of SP 800-53 to develop Appendix F of the ICS version, the original set of controls, enhancements, and supplemental guidance contained in Appendix F were not changed. ICS Supplemental Guidance provides additional guidance on how to apply a control in ICS environments. ICS Enhancements are augmentations to the controls that are required for some ICS. ICS Enhancement Supplemental Guidance provides guidance on how to apply an enhancement in ICS environments.

7 NIST Industrial Control System Security Project, http://csrc.nist.gov/sec-cert/ics/index.html.

FIPS PUB 199 provides standards for categorizing information and information systems based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Categorization considers potential impacts to other organizations and, in accordance with the Patriot Act of 2001 and Homeland Security Presidential Directives, potential national-level impacts in categorizing the information system.

The security controls specified in NIST SP 800-53 are organized into *classes* and *families* for ease of use in the control selection and specification process. There are three general classes of security controls (i.e., management, operational, and technical) and seventeen security control families.[8] Each family contains security controls related to the security functionality of the family. A two-character identifier is assigned to each control family. Table 1 summarizes the classes and families in the security control catalog and the associated family identifiers. The Appendix lists the minimum security controls, or security control baselines, for low-impact, moderate-impact, and high-impact information systems, as determined by applying the criteria in FIPS 199.

Table 1. Security Control Classes, Families, and Identifiers

IDENTIFIER	FAMILY	CLASS
AC	Access Control	Technical
AT	Awareness and Training	Operational
AU	Audit and Accountability	Technical
CA	Certification, Accreditation, and Security Assessments	Management
CM	Configuration Management	Operational
CP	Contingency Planning	Operational
IA	Identification and Authentication	Technical
IR	Incident Response	Operational
MA	Maintenance	Operational
MP	Media Protection	Operational
PE	Physical and Environmental Protection	Operational
PL	Planning	Management
PS	Personnel Security	Operational
RA	Risk Assessment	Management
SA	System and Services Acquisition	Management
SC	System and Communications Protection	Technical
SI	System and Information Integrity	Operational

8 The seventeen security control families in NIST SP 800-53 are closely aligned with the seventeen security-related areas in FIPS PUB 200 specifying the minimum security requirements for protecting federal information and information systems. Families are assigned to their respective classes based on the dominant characteristics of the controls in that family. Many security controls, however, can be logically associated with more than one class. For example, CP-1, the policy and procedures control from the Contingency Planning family, is listed as an operational control but also has characteristics that are consistent with security management.

System Description

As do most major liquid pipeline operators, Olympic used a SCADA system to monitor, operate, and control its pipeline. Figure 2, from NIST SP 800-82, shows the components and general configuration of a SCADA system. The control center houses a control server (MTU) and the communications routers. A typical SCADA system consists of field sensors and actuators, remote terminal units (RTUs), a communications link, and the main SCADA computer. Field sensors and actuators include pumps, valves, pressure transducers, temperature monitors, flow meters, and other devices for the measurement of field data and the signal input/output to those devices.

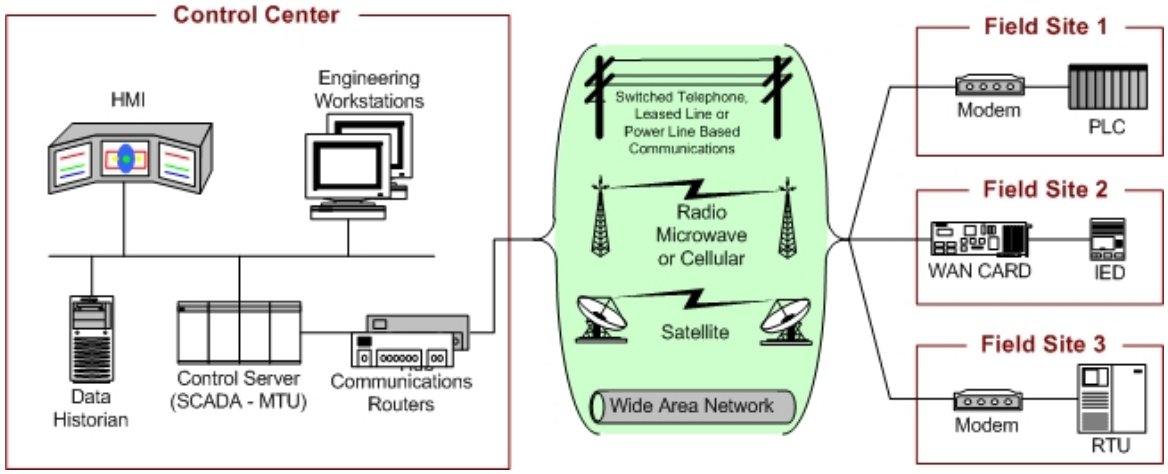

Figure 2. SCADA System General Layout

In a SCADA system, RTUs collect signals from the field hardware and convert them to digital signals for transmission to the control center. RTUs also receive control signals from the SCADA computer and relay them to the individual field sensors. Programmable logic controllers (PLCs) are often used in place of, or in addition to, RTUs. A communications link transmits data to and from the host computer to the field hardware. Traditional SCADA communications methods include leased telephone lines, dial-up telephone lines, and cellular, satellite, and microwave circuits. Pipeline conditions are displayed to the operators, and alarms are generated when field conditions exceed preset levels. In addition to pipeline operators, data users can be accounting personnel, computer technicians monitoring the system, students attending training classes, and computer personnel developing new modules or models.

The Olympic Pipeline SCADA system consisted of Teledyne Brown Engineering SCADA Vector software, version 3.6.1, running on two Digital Equipment Corporation (DEC) VAX Model 4000-300 computers with VMS operating system Version 7.1. (Since the accident, Teledyne Brown has become part of METSO Automation, a SCADA system provider based in Calgary, Canada.) In addition to the two main SCADA computers (OLY01 and OLY02), a similarly configured DEC Alpha 300 computer running Alpha/VMS was used as a host for the separate Modisette Associates, Inc., pipeline leak detection system software package.

The Olympic system was configured with both RTUs and PLCs for the collection of field data. At the time of the accident, most of Olympic's field units also had local controllers embedded in their hardware that were designed to protect the station equipment and downstream piping if contact was lost with the main SCADA computer. Olympic's SCADA communications link between the main computer and the field sensors and controllers was a combination of leased telephone lines and more advanced frame relay service, both of which were provided by local utilities. The communications link did not experience any service problems on the day of the accident. A communications subprocess within the SCADA computer polled field devices every 3 to 7 seconds over the communications link. This subprocess stored the incoming data so that it could be accessed by different SCADA system users. This "working" database was in the physical memory of the SCADA computer as well as on the computer's hard disk. In the event of a SCADA system failure, the SCADA computer could read the hard disk database and begin operations where it had left off before the failure. The display and control subprocesses routed the data to the controllers' screens and the commands the controllers sent to the field devices. Preprogrammed screens were available on any of the computer workstations to display pressure trends or other data in a variety of formats. More than 40 of these preprogrammed screens had been created for Olympic's system, but each workstation was only capable of displaying one such screen at a time. Not all features available in the SCADA software had been implemented.

A number of terminals and workstations other than those used by pipeline controllers were connected to Olympic's VAX system either through network connections or via modem using one of the several serial communications ports located on the two computers. Most of the day-to-day system support and development work was done using one of these remote terminals. The system did not create a keystroke record of the commands entered via one of the remote terminals or workstations. Direct dial-in access to the VAX computer was available from the outside, provided the user knew the phone number and had an authorized dial-up account and system password. The VAX computers hosting the SCADA system, the control room terminals, and workstations and the leak detection computer were connected via an Ethernet backbone network. Each device was connected to one common connection and there was only one path from any one device to another. A bridge connected the Ethernet in the SCADA control room with the company's administrative computer network, which was connected to the Internet. The bridge device offered some protection and isolation of the pipeline control from the administrative segments of the networks. This protection was primarily intended to guard against hardware network failures and faults. Although it also offered some protection against a casual intruder gaining access to the network, it did not offer protection equivalent to that of a full-featured intrusion firewall. No virus protection or access monitoring were incorporated into the system.

The VAX-VMS was designed to be a multi-user system and was capable of keeping track of hundreds of simultaneous users. Each user was allocated his/her share of system resources, and each user was only permitted to run or view files associated with that person's user identification (login). Extensive operating system accountability and permission logs documented the resources used by any user. Only one login was employed by all of the Olympic operators, which allowed all the operators to have undifferentiated system administrator privileges, including manipulation or deletion of

any file on the system (this configuration feature may have played a part in the cyber security event and associated investigation).

In the Olympic SCADA configuration, one computer functioned in a primary node, the other as a backup. The primary computer constantly communicated with the backup to make sure that both computers had the same data. The backup computer was designed to function as a "hot spare" that could seamlessly assume the primary role (with a current database) if necessary. The two computers switched roles once a week, when the operating primary system was intentionally shut down to bring the backup online for the next week. The Vector SCADA system was designed to provide disk records of data that were used by the system and of all the commands issued (this feature played a role in the investigation).

At midnight each day, the system created a complete set of historical records for that day. As the system continued to operate, these files were appended with the new data until midnight, when the appended records became the historical record for that day. The Olympic system was set up with the default VMS system file attributes. The file system allowed Read, Write, Execute and Delete (R,W,E,D) file access for System, Owner , Group and World (S,O,G,W) user categories. It was also possible to add special access control entries (ACEs) to files. VMS had extensive configurable auditing capabilities.

The system would not overwrite older versions of a file but would create a new file with a different version number. The number of versions kept was an account-specific parameter, and the default was usually set to 3. VMS kept a record of all files created or modified, and a file purge could only be accomplished by the creator of the file or by a user with the appropriate system privileges. VMS was designed to log all system operations, errors, and hardware failures. Each entry in the log contained a short descriptive message along with the system time and date.

VMS also contained a security log that kept a record of who was logged into the system. The security log would contain an entry if someone had attempted to break into the operating system. Each time a user typed an incorrect user name or password, a break-in entry would be made in the security log. VMS, by default, allowed the user six attempts to enter the correct password. If a valid password was not entered in the six tries, that particular account was locked out for a period of time. The system was designed to thwart dictionary and other likely password attacks. Additional information is available in the *OpenVMS Guide to System Security* at http://h71000.www7.hp.com/doc/732FINAL/aa-q2hlg-te/aa-q2hlg-te.PDF. Note, however, that Open VMS contains features not necessarily present in the VAX-VMS release used by Olympic.

Olympic made daily backup tapes of all new and modified files found in the SCADA system for both OLY01 and OLY02 computers. This backup was done at about 6:00 a.m. and was accomplished while the systems were operating. A weekly backup of the entire Vector system was made of both machines every Monday. This Monday backup coincided with the weekly alternating of primary and backup computers.

The Accident

A number of events and conditions set the stage for the pipeline rupture. The first event, chronologically, was external damage, gouges, and dents to the pipeline in the vicinity of the eventual rupture. This damage might have been caused in 1993 or 1994 by the actions of a contractor installing water lines across Olympic's pipeline in the vicinity of the rupture. Olympic conducted a cursory investigation of this incident and was aware that damage probably weakened the pipeline and made it susceptible to failure under pressures that an undamaged pipe could probably have withstood.

Second was the construction and startup of the Bayview products terminal. During construction of the terminal, pressure relief valves were installed that were later found to be improperly configured or adjusted, and the actions taken by the company to test and correct the valve settings now seem to have been ineffective.

Finally, on the day of the accident, the SCADA system that controllers used to operate the pipeline became unresponsive, making it difficult for controllers to analyze pipeline conditions and make timely responses to operational problems.

SCADA System Performance

After the Bayview products terminal became operational in December 1998, controllers began to experience difficulties that often involved pressure increases within Bayview, causing the inlet block valve upstream of Bayview to close, thus shutting down the pipeline. Between December 1998 and June 1999, when the accident occurred, the inlet block valve closed 41 times because of high pressure at Bayview. On each occasion when the inlet block valve closed unexpectedly, controllers were able to take some action that kept the pressure across the weakened section of pipeline below that which later caused the pipe to rupture. During 13 (32 percent) of these events, pressure upstream of the closed valve exceeded 1,000 pound per square inch gauge (psig). The highest pressure recorded upstream of the closed valve was 1,339 psig, which was less than the 1,500 psig maximum pressure reached on the day of the rupture.

Higher than normal pressures and higher stress concentrations in the vicinity of the external damage to the pipeline both increased the likelihood of deformations and cracking that could have led to a pipeline rupture. However, because the rupture was later determined to be an overstress separation, with no indications of pipe fatigue, the pipeline likely would not have ruptured on the day of the accident had a pressure spike not occurred. The NTSB concluded that if the SCADA system computers had remained responsive to the commands of the Olympic controllers, the controller operating the pipeline probably would have been able to initiate actions that would have prevented the pressure increase that ruptured the pipeline. In other words, **the unresponsiveness of the SCADA system was determined to be the proximate cause of the rupture.**

Timeline

The following list of events may help keep track of the events that occurred June 10, 1999, when the pipeline owned by Olympic Pipeline Company ruptured and gasoline leaked into two creeks in Bellingham, Washington.

3:00 p.m. – Controller changed gasoline delivery points. System administrator working on OLY-02 SCADA historical database entered two new records.
3:10 p.m. – SCADA computer began to generate error messages related to the historical database. System administrator checked the checked the records and left for 15 minutes.
3:18 p.m. – SCADA OLY-02 became erratic and at one point non-responsive.
3:24 p.m. – SCADA OLY-02 was taken offline.
3:27 p.m. – Backup SCADA OLY01 was brought online.
3:28 p.m. – Pipeline ruptured.
3:44 p.m. – SCADA OLY-02 was back online.
3:48 p.m. – SCADA OLY-02 was operational after new records were deleted.
4:04 p.m. – SCADA OLY-01 was back on standby mode.
4:16 p.m. – Pipeline flow was restarted.
4:29 p.m. – Leak detection alert was issued.

Investigation, Analysis, and Observations

Investigators attempted to determine why the SCADA system, which was not reported to have experienced operational problems since November 1998, became slow or unresponsive at a critical time during the pipeline operations on June 10, 1999. Key pipeline company personnel have refused to respond to NTSB questions, exercising their Fifth Amendment rights. Those individuals include two controllers who were on duty at the time of the accident, their supervisor, and a former controller acting as system administrator responsible for maintaining the SCADA system and acting as a relief controller.

At about 3:00 p.m., the controller, using the SCADA system, began preparing to discontinue product delivery to the Tosco facility and initiate delivery of gasoline to ARCO's Harbor Island terminal in Seattle, Washington. At about the same time, the system administrator was working on a terminal in the control center computer room. It is believed that he was programming some new reports that extracted data from the SCADA historical database. At about 3:10 p.m., the SCADA computer began to generate error messages related to the historical database. The system administrator checked the format of the new records and found no errors; thus, he believed something other than the new records was causing the problem. He then left the control room for 15 minutes.

At the time of the accident, the SCADA system was unresponsive to the commands of the controllers. Had the controller been able to start the pump at the Woodinville station, it is probable that the pressure backup would have been alleviated and the pipeline operated routinely for the balance of the fuel delivery. The controller attempted to systematically slow or shut down the line, as evidenced by his call to the electrician at the Allen station to locally shut down one of the pumps. Even if the controller had been unable to prevent

the pressure buildup and the subsequent closure of the inlet block valve at Bayview, had he had full SCADA system control he may have been able to reduce the flow through the pipeline sufficiently to minimize the severity of the pressure increase when the block valve did close.

When the system administrator returned, he reported the primary computer as unresponsive. In addition, he stated that the console terminal did not respond to his commands, including the attempt to start the Woodinville pump from the SCADA system. The controllers were reporting that the SCADA system was not updating the control screens like it normally does. The SCADA system normally polls remote locations to collect field data points on a continuous basis, usually collecting fresh data every 5-7 seconds. There was a noticeable change in the polling pattern immediately prior, during, and immediately after the pipe rupture. At that point, the system administrator should have followed policy and procedure (had there been any) to notify the appropriate personnel that the computer was acting abnormally. Instead, after checking the records he had entered and finding no problems with them, he left the computer room and did not return for about 15 minutes. If the controller had been notified promptly at 3:10 p.m. that the SCADA system appeared to be malfunctioning, he may have responded differently before initiating the switch of delivery points. Also, if the control center supervisor had been notified promptly, he may have been able to quickly restore the computers to normal operations (as he did 30 minutes later).

The SCADA problems grew more pronounced over the next 20 minutes, during which, at one point, the system became completely unresponsive. This period of non-responsiveness coincided with the rupture of the pipeline at about 3:28 p.m. The SCADA problems encountered by the controllers occurred shortly after the system administrator inserted new records into the system computer and were resolved after the control center supervisor deleted the new records. Also, the system administrator said that as the new records were being deleted, he noticed a typographical error in the records that had not been there when the records were checked earlier. Because of this and the fact that the SCADA system had not previously exhibited a similar non-responsiveness, the NTSB concluded that the degraded SCADA performance witnessed by the pipeline controllers on the day of the accident likely resulted from the database development work that was done on the SCADA system.

Equilon, a joint venture between Texaco and Shell, was the majority owner of Olympic Pipeline at the time of the accident. Equilon had a SCADA development center in Houston, Texas. Consequently, Equilon supported Olympic in the analysis of the SCADA system performance. A tape of software used on the Olympic system was shipped to Houston to allow the Olympic system to be reproduced at the development site. Subsequent analysis and testing performed by Olympic and Equilon, working in conjunction with the SCADA software vendor, did not identify any coding within the SCADA software that would have caused the system anomalies encountered on the day of the accident. The testing data did not uncover any problems in the error-handling routines that would place demands on system resources in excess of the reserve processing capacity.

SCADA system data acquisition is accomplished by scanning the field inputs connected to the RTU and/or PLC. The data is usually collected at a polling rate configured by the operator. The polling rate is determined by the number of sites, the amount of data at each site, the maximum bandwidth of the communication channel and the minimum required display and control time. Once the data has been acquired by the field equipment, it is sent to the SCADA Host where the SCADA software will scan the acquired data (in this case, a nominal 5-7 second scan rate.) The data is then processed to detect preset alarm conditions, and if an alarm is present, an alarm message will flash on the operator screen and added to an alarm list. The operator must then acknowledge this alarm.

The scan rate is a measure of the response of the SCADA system to changes in field conditions. Consequently, a slower response reduces the ability of the SCADA system to automatically respond and provide operator information to system changes. As shown in figure 3, from 3:07 PM to 3:20 PM and from 3:50 PM on, the SCADA scan rate response appears normal. However, there was a significant change in the polling pattern prior to (3:18 PM to 3:28 PM) and after the pipe rupture (3:28 PM to 3:50 PM). Ironically, the scan rate appears normal at the time of the event (3:28 PM). The start of the slowdown coincided with the insertion of new records into the system computer (approximately 8 minutes after initial error messages) and appears to have been resolved sometime after the control center supervisor deleted the new records (approximately 6 minutes later). The longer, erratic scan rate reduced the ability of the SCADA to respond to rapid system changes and also reduced operator confidence in the data being monitored.

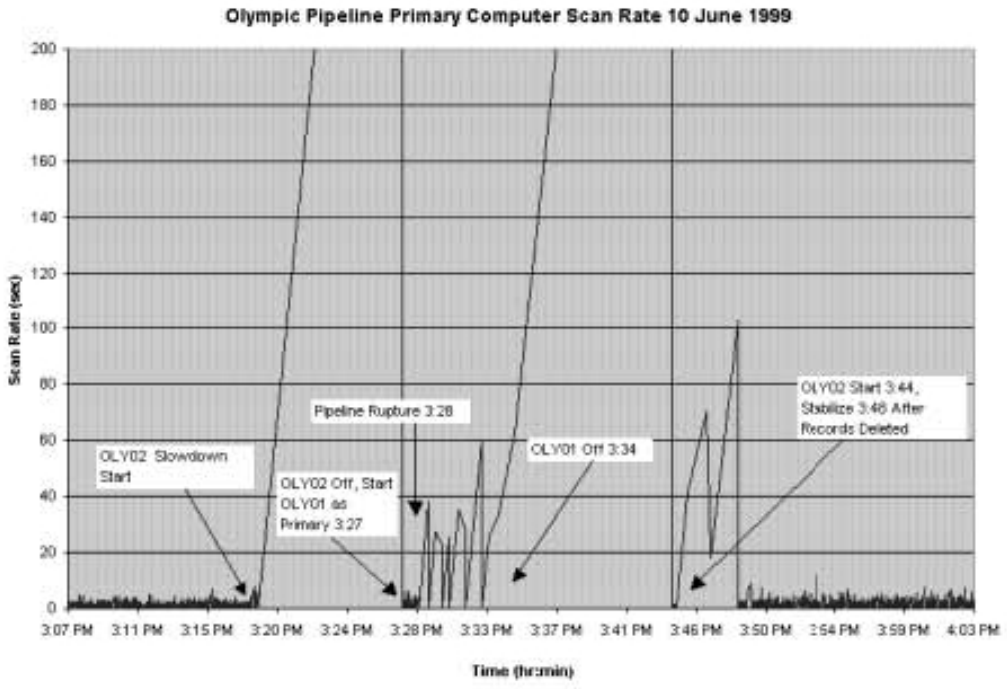

Figure 3. SCADA Response

Records with known errors were repeatedly input into the historical database, but the computer slowdown of June 10, 1999, could not be replicated. Because the problems the

SCADA system experienced on the day of the accident could be neither explained nor replicated after the accident, the exact fault in the historical database that initiated the system's failure on the day of the accident will probably never be known.

The attempts to determine the cause of the SCADA system slowdown were hampered in that the system used for testing was not a clone of the operational system. The source code for the Historic process in the software used by the Olympic computer system was significantly different than anticipated. Computer hardware was not available that matched the performance of the existing Olympic system, so the testing was performed on a system that was slightly smaller and slower. Normal loading of the data acquisition could not be completely accomplished, so the load was tested with simulated traffic of 30% of the number of RTUs in service, with the scan times raised 600% to simulate a full load. Furthermore, the records entered just before the slowdown had been deleted to stop the abnormal computer operations. For the same reason, the effect, if any, of the processing capacity of the SCADA computers on the slowdown cannot be determined. As noted earlier, the system administrator was working on the live system.

Even though the SCADA system was configured to permit alterations to be made to the historical database while the system was online, the NTSB did not consider this practice to be prudent. The NIST SP 800-53 ICS supplemental guidance supports this position. Computer systems, while they have proven their worth in all modes of transportation, are not infallible, nor are their operators and administrators. Newly developed computer routines do not always work correctly at first and must be revised. Sometimes, seemingly simple mistakes can result in catastrophic consequences, even on the most robust of operating systems. Olympic personnel used the operational system as a test bed to develop changes and upgrades to the database without first testing the changes on a separate offline system.

The VAX-VMS system that was used as the platform for Olympic's SCADA system was a multi-user system, but all authorized Olympic computer operators used the same login. Thus, even though the operating system could track individual users, the system had no means of distinguishing one user from another. This single-login policy severely limited the ability of the company to audit the system or to assign individual accountability for actions performed on the VAX or SCADA system. Furthermore, all authorized users had system administrator privileges, allowing them to manipulate or delete any and all of the files contained on the system. Because they all used the same login name, no record of exactly who performed what action was available. The operators refused to testify during the NTSB investigation. Additionally, several important files were inexplicably missing. They included several versions of the Accounting data log files on OLY01 and OLY02 and several versions of the Operator log files on both OLY01 and OLY02. This includes the Operator log from OLY01 that covers the time frame of the reported slowdown.

Another drawback of using one login account is that all users used one system resource setting for all of their activities. VMS has the ability to allocate its resources based on a login's permissions. This feature is implemented in a multi-user system to keep the activities of one user from consuming all of the available system resources. The one account that the Olympic operators were using contained sufficient priority to allocate

any and all available system resources for their task, taking all priority away from the operational pipeline system.

The SCADA system was connected via a bridge to the rest of the building's network. It was also directly accessible via dial-in modem. No firewalls or access monitoring were incorporated into the system. These protections should have been installed to isolate the system from a hacker attack. Although no evidence was found to suggest that an intrusion by an unauthorized or unknown user caused the computer slowdown that occurred on the day of the accident, the lack of basic security features related to the SCADA system could allow such an intrusion in the future.

The NTSB concluded that Olympic did not adequately manage the development, implementation, and protection of its SCADA system.

Since the accident, Olympic took a number of steps to improve its SCADA system's performance, reliability, and security, including increasing computer processing speed and capacity and addressing both physical security of the control center and electronic access security of the SCADA computers. The Olympic Pipeline Company has subsequently gone out of business.

When the delivery points were changed, pressure in the pipeline began to build. According to other controllers interviewed, this was a normal occurrence, and the standard response was to start a second pump at the Woodinville station. This is what the controller attempted to do, but he could not start the pump because of the non-responsiveness of the SCADA system. Because the Woodinville station was unattended, the controller had no timely alternative means of starting a pump there. Without the extra Woodinville pump, pressure continued to build upstream of that station. In an apparent attempt to systematically shut the pipeline down, the controller called an electrician at the upstream Allen station and asked that a pump there be shut down to slow the flow of product toward Woodinville.

Meanwhile, the uncontrolled pressure buildup had begun to reach overpressure protection settings, thus shutting down pumping units along the pipeline and initiating the closure of the inlet block valve at Bayview. This chain reaction effect went virtually unchecked because of the slow response or non-response of the SCADA system. Because of its unresponsiveness, the computer system administrator then shut down the primary SCADA computer in preparation for bringing the backup computer online to maintain SCADA functionality. Approximately 1 minute after the backup OLY01 system was brought online as the primary computer, the pipeline ruptured. At that point, the pipeline had been virtually shut down by the tripping of pumps and the closing of the valve.

About 7 minutes after the rupture, the controller called personnel at the ARCO refinery near Cherry Point and asked that they discontinue pumping gasoline to the Cherry Point station. It is not clear what or how much information was available to the controllers between the time the SCADA system OLY02 was halted and the time it was brought back online and stabilized about 20 minutes later, at about 3:48 p.m. However, none of the readily available information indicated that the pipeline had ruptured. The inlet block

valve upstream of the Bayview terminal had closed repeatedly in the preceding 6 months, and each time, the pipeline had been restarted without incident.

Olympic procedures called for the controller to determine the cause of a pressure change that shuts down a pump by reviewing such data as pressure trends. In the accident, the first pump that failed was one of the boosters at Bayview. NTSB investigators could not determine whether the controller reviewed any pressure trends before restarting the pipeline. Because the SCADA screens for Bayview were still under development (6 months after the facility's startup), no pressure trend SCADA screen for Bayview was readily available to the controller.

Although this pressure trend data was probably not available to the controller until about 4:04 p.m. when the OLY01 computer was restarted, had the controller reviewed this trend (and it is unclear whether he would have done so had it been available), he might have investigated the pressure indications and not restarted the pipeline.

At 4:11 p.m., the controller restarted the pipeline by opening the inlet block valve for Bayview and, a few minutes later, notifying personnel at the ARCO refinery to resume delivery. By taking these actions, the controller significantly increased the amount of gasoline released. The effect of the additional gasoline release on the resulting fire cannot readily be quantified. The fact that the controller called the electrician at the Allen station to verify a pressure reading there indicates that the controller was watching pressures along the pipeline after he restarted it. He probably thought he had a slack line condition, since the only pump still operating after the line shut down was at Woodinville. This assumption would have delayed his recognition that a release had occurred and lessened the perceived validity of any leak detection alert. In taking these actions, the controller was working under the direction of his supervisor, who had approved the restart and who thus also apparently did not believe additional actions to verify the integrity of the pipeline were necessary.

About 4:30 p.m., approximately 13 minutes after the pipeline was restarted, the pipeline leak detection system issued an alert for a possible leak. At about the same time, the control center received a call from an Olympic employee, on his way home from work, who reported the presence of gasoline in Whatcom Creek. Within minutes, the controller had initiated actions to close mainline block valves to isolate the rupture and to stop the transfer of gasoline into the pipeline from ARCO.

Relevant NTSB Accident Board Findings and Recommendations

The following findings and recommendations pertain to cyber security"

1. If the SCADA system computers had remained responsive to the commands of the Olympic controllers, the controller operating the accident pipeline probably would have been able to initiate actions that would have prevented the pressure increase that ruptured the pipeline.

2. The degraded SCADA performance witnessed by the pipeline controllers on the day of the accident likely resulted from the database development work that was done on the SCADA system.
3. Had the SCADA database revisions that were performed shortly before the accident been performed and thoroughly tested on an offline system instead of the primary online SCADA system, errors resulting from those revisions may have been identified and repaired before they could affect the operation of the pipeline.
4. Olympic did not adequately manage the development, implementation, and protection of its SCADA system.

Probable Causes

The NTSB determined the probable causes of the June 10, 1999, rupture of the Olympic pipeline in Bellingham, Washington, were the following:

1. Damage done to the pipe by IMCO General Construction, Inc., during the 1994 Dakin-Yew water treatment plant modification project and Olympic Pipeline Company's inadequate inspection of IMCO's work during the project.
2. Olympic Pipeline Company's inaccurate evaluation of inline pipeline inspection results, which led to the company's decision not to excavate and examine the damaged section of pipe.
3. Olympic Pipeline Company's failure to test, under approximate operating conditions, all safety devices associated with the Bayview facility before activating the facility.
4. Olympic Pipeline Company's failure to investigate and correct the conditions leading to the repeated unintended closing of the Bayview inlet block valve.
5. Olympic Pipeline Company's practice of performing database development work on the SCADA system while the system was being used to operate the pipeline, which led to the system's becoming non-responsive at a critical time during pipeline operations.

Cyber Security Issues

Following a thorough review of the final NTSB report and the interim documentation provided by NTSB[9], the following cyber security issues were adjudged to be present immediately before, during, and shortly after the Bellingham pipe rupture. These issues, taken separately or in combination, could have led to the abnormal SCADA operation or precluded an ability to determine the cause of the event.

1. Unsecured Remote Access
   a. The terminals and workstations were connected to the SCADA system either through network connections or via modems using one of the several serial communications ports located on the two SCADA computer units. Most of the day-to-day system support and development work was done using one of these remote terminals.

9 National Transportation Safety Board, Office of Research and Engineering, *Specialist's Computer Study, SCADA Control System*, Washington, D.C. 20594, April 8, 2002.

b. Direct dial-in access to the VAX computer was available from the outside, provided the user knew the phone number and had an authorized dial-up account and system password.

2. Network Separation
   a. The SCADA host computers, the control room computers, and the leak detection computer were interconnected via a basic Ethernet backbone network. This means that each device was connected to one common connection point and that there was only one path from any one device to another.
   b. A bridge connected the Ethernet in the SCADA control room with the company's administrative computer network.
   c. The administrative computer network was reported to have some Internet connectivity.
   d. It was reported that there were several other departments that used data obtained from the SCADA system.

3. Security Technologies
   a. The system did not create a keystroke record of the commands entered via one of the remote terminals or workstations.
   b. No virus protection or access monitoring was incorporated into the system.
   c. The VMS system was designed to log all system operations, errors, and hardware failures. VMS also contained a security log that kept a record of who was logged into the system. The security log would contain an entry if someone had attempted to break into the computer operating system. Each time a user typed an incorrect user name or password, a break-in entry would be made in the security log. The security log contained no evidence of an unauthorized attempt to access the system.

4. Security Policies
   a. There was no indication of an in-place cyber security program, including control system policies and procedures.
   b. The VAX-VMS system that was used as the platform for Olympic's SCADA system was a multi-user system, but all authorized Olympic computer operators used the same login. Thus, even though the operating system could track individual users, the system had no means of distinguishing one user from another. This single-login policy severely limited the ability of the company to audit the system or to assign individual accountability for actions performed on the VAX or SCADA system. Furthermore, all authorized users had system administrator privileges, allowing them to manipulate or delete any and all of the files contained on the system. Because they all used the same login name, no record of exactly who performed what action was available.
   c. The pressure trend displays during the period that the Olympic SCADA system was experiencing a computer system slowdown and stoppage were presenting potentially misleading data to the operator. There was no special highlighting feature programmed to alert the controllers that they were looking at a graph that may contain gaps in the displayed data.

5. Training
    a. The computer system support person was formerly a full-time pipeline controller. Although appearing well versed in SCADA technology, he had not received any training in the operating system or SCADA applications.
    b. There was no mention of any computer security training provided or taken by any of the staff.

6. Forensics
    a. The Equilon software support group performed a review of the pipeline control software after the pipe rupture event. In an attempt to replicate the SCADA computer performance anomaly, an image copy of the disk was installed on one of the Equilon development computers. The Equilon development system and software were different from the Olympic SCADA system. No performance anomalies could be created on the Olympic system running on the Equilon computer.
    b. Key logs were inexplicably missing, including during the period when the SCADA was unresponsive.
    c. The SCADA operator refused to testify.

Recommendations

As a result of its investigation of the June 10, 1999, rupture of an Olympic Pipe Line Company pipeline in Bellingham, Washington, the NTSB made the following safety recommendations:

1. Issued an advisory bulletin to all pipeline operators who use SCADA systems advising them to implement an offline workstation that can be used to modify their SCADA system database or to perform developmental and testing work independent of their online systems.
2. Advised operators to use the offline system before any modifications are implemented to ensure that those modifications are error-free and that they create no ancillary problems for controllers responsible for operating the pipeline.

NIST SP 800-53 Controls

FIPS PUB 199 provides standards for categorizing information and information systems based on the potential impact on an organization should certain events occur which could jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. FIPS PUB 199 defines three categories of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). The potential impact is HIGH if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might cause any of the following events:

1. A severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions
2. Major damage to organizational assets
3. Major financial loss
4. Severe or catastrophic harm to individuals, involving loss of life or serious life-threatening injuries

A breach of the SCADA system-controlled pipeline clearly fits into the HIGH category.

Table A-1 in the Appendix lists all of the controls specified in NIST SP 800-53, identifying which controls are included in the three baseline sets. The controls that directly address cyber security flaws and weaknesses identified in the Bellingham incident are discussed below.

Policies and Procedures

The first control in every control family addresses policies and procedure. With minor variations, the control begins: "The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate …." Although enumerated for each control family, the family policy can be included as part of the general information security policy for the organization. Family control procedures can be developed for the security program in general and for a particular information system, when required. The control information discussed in this section was extracted from NIST SP 800-53.

Access Control

Access control is concerned with mediating the ability of subjects or initiators to use information objects or targets within the information system. The process of determining which use of resources is permitted and, where appropriate, preventing unauthorized access is called *access control*. Modes of use, or access, typically include read, write, append, and execute. Access control can only be provided within the context of a defined security policy. Table 2 shows the Access Control family (AC) controls that can be used to establish and implement such policy:

Table 2. Available Access Controls

AC-1	Access Control Policy and Procedures	AC-11	Session Lock
AC-2	Account Management	AC-12	Session Termination
AC-3	Access Enforcement	AC-13	Supervision and Review—Access Control
AC-4	Information Flow Enforcement	AC-14	Permitted Actions without Identification or Authentication
AC-5	Separation of Duties	AC-15	Automated Marking
AC-6	Least Privilege	AC-16	Automated Labeling

AC-7	Unsuccessful Login Attempts	AC-17	Remote Access
AC-8	System Use Notification	AC-18	Wireless Access Restrictions
AC-9	Previous Logon Notification	AC-19	Access Control for Portable and Mobile Devices
AC-10	Concurrent Session Control	AC-20	Use of External Information Systems

Use of the following controls could have alleviated many of the access-related problems at Olympic:

1. **AC-2 ACCOUNT MANAGEMENT**: "The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts…."
2. **AC-3 ACCESS ENFORCEMENT**: "The information system enforces assigned authorizations for controlling access to the system in accordance with applicable policy."
3. **AC-5 SEPARATION OF DUTIES**: "The information system enforces separation of duties through assigned access authorizations,"
4. **AC-6 LEAST PRIVILEGE**: "The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks."

ICS Supplemental Guidance includes the following information: "Account management may include additional account types (e.g., role based, device based, attribute based). The organization removes, disables, or otherwise secures default accounts (e.g., maintenance). Default passwords are changed. In cases where physical access to the workstation, hardware, and/or field devices predefine privileges, the organization implements physical security policies, and procedures based on organization risk assessment…."

AC-5 SEPARATION OF DUTIES specifies that "…the information system enforces separation of duties through assigned access authorizations." **AC-6 LEAST PRIVILEGE** specifies that "…the information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks." ICS Supplemental Guidance advises that "…in situations where the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety, reliability) to implement separation of duties (for example, the organization has a single individual to perform all roles or the ICS does not differentiate roles), the organization documents the rationale for not implementing the control, documents appropriate compensating security controls in the System Security Plan, and implements these compensating controls."

The applicable NIST SP 800-53 control for remote access is AC-17 REMOTE ACCESS. The statement of the control is: "The organization authorizes, monitors, and controls all methods of remote access to the information system." ICS Supplemental Guidance includes the following: "Examples of remote access methods include dial-up, broadband, and wireless... The organization restricts access achieved through dial-up connections

(e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections… Remote access to ICS component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated…."

Use of these controls could have mitigated many of the access control-related deficiencies noted:

- All authorized Olympic computer operators used the same login.
- All authorized users had system administrator privileges.
- All users used one system resource setting for all of their activities.

Audit and Accountability

The Audit and Accountability family (AU), shown in table 3, contains controls that can be used to maintain a record of important events which are significant and relevant to the security of the information system:

Table 3. Available Audit and Accountability Controls

AU-1	Audit and Accountability Policy and Procedures	AU-7	Audit Reduction and Report Generation
AU-2	Auditable Events	AU-8	Time Stamps
AU-3	Content of Audit Records	AU-9	Protection of Audit Information
AU-4	Audit Storage Capacity	AU-10	Non-repudiation
AU-5	Response to Audit Processing Failures	AU-11	Audit Record Retention
AU-6	Audit Monitoring, Analysis, and Reporting		

The applicable NIST SP 800-53 control for recording keystrokes, and any other security-relevant data, is AU-2 AUDITABLE EVENTS. The statement of the control is deceptively simple: "The information system generates audit records for the following events: [*Assignment: organization-defined auditable events*]." Assignments are provided in NIST SP 800-53 so that the organization can customize the controls.

ICS Supplemental Guidance begins as follows: "The purpose of this control is to identify important events which need to be audited as significant and relevant to the security of the information system. The organization specifies which information system components carry out auditing activities. Auditing activity can affect information system performance. Therefore, the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations…."

Additional ICS Supplemental Guidance is provided: "Most ICS audit at the application level. Some ICS may not have this ability. In situations where the organization determines it is not feasible or advisable (e.g., adversely impacting performance, safety,

reliability) to implement auditable events, the organization documents the rationale for not implementing the control, documents appropriate compensating security controls in the System Security Plan, and implements these compensating controls."

AU-9 PROTECTION OF AUDIT INFORMATION requires that the information system must protect audit information and audit tools from unauthorized access, modification, and deletion.

These controls could have assured the availability of records, in contrast to what happened:

- Several important files were inexplicably missing:
  - Several versions of the Accounting data log files on OLY01 and OLY02
  - Several versions of the Operator log files on both OLY01 and OLY02, including the Operator log from OLY01 covering the time frame of the reported slowdown

Creating a keystroke record of the commands entered via one of the remote terminals or workstations could have been specified under AU-2.

Awareness and Training

A strong cyber security program cannot be put in place without significant attention given to training agency IT users on security policy, procedures, and techniques, as well as the various management, operational, and technical controls necessary and available to protect IT resources. In addition, those in the agency who manage the IT infrastructure need to have the necessary skills to carry out their assigned duties effectively. The Awareness and Training (AT) family contains the controls shown in table 4:

Table 4. Available Awareness and Training Controls

AT-1	Security Awareness and Training Policy and Procedures	AT-4	Security Training Records
AT-2	Security Awareness	AT-5	Contacts with Security Groups and Associations
AT-3	Security Training		

AT-2 SECURITY AWARENESS and **AT-3 SECURITY TRAINING** address all information system users and personnel who have significant information system security roles and responsibilities, respectively: "The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access."

Certification, Accreditation, and Security Assessments

The Certification, Accreditation, and Security Assessments controls shown in table 5 are concerned with determining the extent to which the other controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system:

Table 5. Available Audit and Accountability Controls

CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-5	Plan of Action and Milestones
CA-2	Security Assessments	CA-6	Security Accreditation
CA-3	Information System Connections	CA-7	Continuous Monitoring
CA-4	Security Certification		

CA-2 SECURITY ASSESSMENTS includes the following ICS Supplemental Guidance: "The organization ensures that assessments do not interfere with ICS functions. The assessor fully understands the corporate cyber and ICS security policies and procedures and the specific health, safety, and environmental risks associated with a particular facility and/or process. A production ICS may need to be taken off-line, or replicated to the extent feasible, before the assessments can be conducted. If an ICS must be taken off-line for assessments, assessments are scheduled to occur during planned ICS outages whenever possible. In situations where the organization determines it is not feasible or advisable (e.g. adversely impacting performance, safety, reliability) to implement the live testing of the production ICS, the organization documents the rationale for using a replicated system."

Configuration Management

NIST SP 800-53 defines *Configuration Control* as the "process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation…" and provides the controls listed in table 6:

Table 6. Available Configuration Management Controls

CM-1	Configuration Management Policy and Procedures	CM-5	Access Restrictions for Change
CM-2	Baseline Configuration	CM-6	Configuration Settings
CM-3	Configuration Change Control	CM-7	Least Functionality
CM-4	Monitoring Configuration Changes	CM-8	Information System Component Inventory

CM-3 CONFIGURATION CHANGE CONTROL specifies that, "…the organization authorizes, documents, and controls changes to the information system." ICS Control Enhancements add, "…the organization tests, validates and documents changes (e.g. patches and updates) before installing them on the operational ICS." However, this Control Enhancement is not included in the HIGH baseline.

CM-4 MONITORING CONFIGURATION CHANGES specifies that, "…the organization monitors changes to the information system conducting security impact analyses to determine the effects of the changes." Supplemental Guidance is provided: "Prior to change

implementation, and as part of the change approval process, the organization analyzes changes to the information system for potential security impacts. After the information system is changed (including upgrades and modifications), the organization checks the security features to verify that the features are still functioning properly. The organization audits activities associated with configuration changes to the information system." ICS Supplemental Guidance adds: "The organization considers ICS safety and security interdependencies."

CM-5 ACCESS RESTRICTIONS FOR CHANGE specifies that: "the organization: (i) approves individual access privileges and enforces physical and logical access restrictions associated with changes to the information system; and (ii) generates, retains, and reviews records reflecting all such changes."

These controls would have elevated risks due to alterations to be made to the historical database while the system was online, and using the operational system as a test bed to develop changes and upgrades to the database without first testing the changes on a separate offline system.

Contingency Planning

Contingency planning controls, shown in table 7, are concerned with restoring the system after a disruption or failure:

Table 7. Available Contingency Planning Controls

CP-1	Contingency Planning Policy and Procedures	CP-6	Alternate Storage Site
CP-2	Contingency Plan	CP-7	Alternate Processing Site
CP-3	Contingency Training	CP-8	Telecommunications Services
CP-4	Contingency Plan Testing and Exercises	CP-9	Information System Backup
CP-5	Contingency Plan Update	CP-10	Information System Recovery and Reconstitution

The applicable NIST SP 800-53 control for isolating control and administrative networks is **CP-2 CONTINGENCY PLAN**. The statement of the control is: "The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel."

The statement of the control is: "The organization develops and implements a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel."

ICS Supplemental Guidance includes: "The organization defines contingency plans for categories of disruptions or failures. In the event of a loss of processing within the ICS or communication with operational facilities, the onsite ICS components should be capable of executing predetermined procedures…."

Incident Response

Organizational policy and procedure governs appropriate behavior when confronted with anomalous behavior. Incident response controls are listed in table 8:

Table 8. Available Incident Response Controls

IR-1	Incident Response Policy and Procedures	IR-5	Incident Monitoring
IR-2	Incident Response Training	IR-6	Incident Reporting
IR-3	Incident Response Testing and Exercises	IR-7	Incident Response Assistance
IR-4	Incident Handling		

FIPS PUB 200 defines an incident as, "An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies." Once it has been determined that an incident exists, the Incident Response (IR) family in NIST SP 800-53 applies.

Identifying the cause of anomalous behavior is part of after-the-fact computer forensics. The organization should provide the operators, other persons in sensitive operational positions in particular, and all employees in general with definitions of levels of anomalous behavior of the SCADA system and the procedures to follow when anomalous behavior is observed. In this case, highly trained specialists in the SCADA system and cyber security should have been notified.

All controls in the IR family could have alleviated the incident. Following an appropriate set of incident response policies and procedures when the non-responsiveness of the SCADA system was observed could have prevented the rupture.

Media Protection

The scope of media continues to widen as technology advances. Information system media include both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, and digital video disks) and non-digital media (e.g., paper, microfilm). Media protection controls, listed in table 9, control also applies to portable and mobile computing and communications devices with information storage capability (e.g., notebook computers, personal digital assistants, cellular telephones):

Table 9. Available Media Protection Controls

MP-1	Media Protection Policy and Procedures	MP-4	Media Storage
MP-2	Media Access	MP-5	Media Transport
MP-3	Media Labeling	MP-6	Media Sanitization and Disposal

The Media Protection family (MP) in NIST SP 800-53 contains six controls. The most general is **MP-4 MEDIA STORAGE**, which states, "The organization physically controls and securely stores information system media within controlled areas." **MP-2 MEDIA ACCESS** states, "The organization restricts access to information system media to authorized individuals." Supplemental guidance includes, "An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access."

System and Communications Protection

The system and communications controls, listed in table 10, protect the executable programs and the data exchanged outside these processes:

Table 10. Available System and Communications Controls

SC-1	System and Communications Protection Policy and Procedures	SC-13	Use of Cryptography
SC-2	Application Partitioning	SC-14	Public Access Protections
SC-3	Security Function Isolation	SC-15	Collaborative Computing
SC-4	Information Remnance	SC-16	Transmission of Security Parameters
SC-5	Denial of Service Protection	SC-17	Public Key Infrastructure Certificates
SC-6	Resource Priority	SC-18	Mobile Code
SC-7	Boundary Protection	SC-19	Voice Over Internet Protocol
SC-8	Transmission Integrity	SC-20	Secure Name /Address Resolution Service (Authoritative Source)
SC-9	Transmission Confidentiality	SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)

SC-10	Network Disconnect	SC-22	Architecture and Provisioning for Name/Address Resolution Service
SC-11	Trusted Path	SC-23	Session Authenticity
SC-12	Cryptographic Key Establishment and Management		

The applicable NIST SP 800-53 control for isolating control and administrative networks is **SC-7 BOUNDARY PROTECTION**. The statement of the control is: "The information system monitors and controls communications at the external boundary of the information system and at key internal boundaries within the system." The Olympic system did not employ boundary protection.

The Supplemental Guidance includes the following: "Examples of remote access methods include dial-up, broadband, and wireless... The organization restricts access achieved through dial-up connections (e.g., limiting dial-up access based upon source of request) or protects against unauthorized connections or subversion of authorized connections…." ICS Supplemental Guidance includes: "Remote access to ICS component locations (e.g., control center, field locations) is only enabled when necessary, approved, and authenticated…."

Use of the above controls could have improved the observed deficiencies:

- The SCADA system was connected to the rest of the building's network.
- The SCADA system was accessible via dial-in modem.
- No firewalls had been implemented.
- Weak boundary protection was in place, provided by a bridge connecting the control room to the company's administrative network.

System and Information Integrity

FIPS PUB 199 quotes the definition of integrity as follows: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…." [44 U.S.C., Sec. 3542], observing that. "…a loss of *integrity* is the unauthorized modification or destruction of information." The system and information integrity control family includes the controls listed in table 11:

Table 11. Available System and Information Integrity Controls

SI-1	System and Information Integrity Policy and Procedures	SI-7	Software and Information Integrity
SI-2	Flaw Remediation	SI-8	Spam Protection

SI-3	Malicious Code Protection	SI-9	Information Input Restrictions
SI-4	Information System Monitoring Tools and Techniques	SI-10	Information Accuracy, Completeness, Validity, and Authenticity
SI-5	Security Alerts and Advisories	SI-11	Error Handling
SI-6	Security Functionality Verification	SI-12	Information Output Handling and Retention

The applicable NIST SP 800-53 control for protection against viruses and other kinds of malicious code is **SI-3 MALICIOUS CODE PROTECTION**. The statement of the control is: "The information system implements malicious code protection." The ICS Supplemental Guidance includes: "The organization employs malicious code protection mechanisms at critical information system entry and exit points (e.g., firewalls, electronic mail servers, web servers, proxy servers, remote-access servers) and at workstations, servers, or mobile computing devices on the network. The organization uses the malicious code protection mechanisms to detect and eradicate malicious code (e.g., viruses, worms, Trojan horses, spyware) transported: (i) by electronic mail, electronic mail attachments, Internet accesses, removable media (e.g., USB devices, diskettes or compact disks), or other common means; or (ii) by exploiting information system vulnerabilities." No malicious code protection was employed.

SI-7 SOFTWARE AND INFORMATION INTEGRITY specifies, "The information system detects and protects against unauthorized changes to software and information." The efficacy of this control depends on the definition of unauthorized changes, such as programming the operational system. See also Configuration Management.

The above controls could have mitigated the following deficiency that was noted:

- No virus protection was in place.

Conclusions

The SCADA system was integral to maintaining safe operation of the pipeline. However, various factors contributed to the inoperability of the SCADA system and the lack of adequate response to the inoperable SCADA system at critical times. A comprehensive control system cyber security program was not in place nor was appropriate SCADA operator training. The SCADA system appeared to have diagnostics capabilities, but those capabilities were not configured to address internal cyber issues. In addition, system logs that should have been automatically generated were inexplicably missing. The single backbone Ethernet network did not provide adequate separation from the real-time systems and non-critical business networks. Finally, the interconnections between the SCADA system and the plant leak detection system did not provide for adequate resources or separation.

Appendix. Minimum Security Control Baselines

NIST SP 800-53 provides a catalog of security controls and baseline starting points based on FIPS 199 impact categorization. Agencies perform an organizational risk assessment to consider additional threat information, specific mission requirements, operating environments, and any other factors that might affect accomplishment of the agency's mission or business functions, and can add appropriate security controls or enhancements from the SP 800-53 catalog or create new controls if necessary. Understanding the baseline control sets is the first step in implementing cyber security management, operational, and technical safeguards.

Table A-1 lists the minimum security controls, or security control baselines, for LOW-impact, MODERATE-impact, and HIGH-impact information systems. The three security control baselines are hierarchical in nature with regard to the security controls employed in those baselines. If a security control is selected for one of the baselines, the family identifier and control number are listed in the appropriate column. If a control is not used in a particular baseline, the entry is marked "not selected." Control enhancements, when used to supplement basic security controls, are indicated by the number of the control enhancement.

Table A-1. NIST SP 800-53 Security Control Baselines

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
Access Control				
AC-1	Access Control Policy and Procedures	AC-1	AC-1	AC-1
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Access Enforcement	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Information Flow Enforcement	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	Not Selected	AC-5	AC-5
AC-6	Least Privilege	Not Selected	AC-6	AC-6
AC-7	Unsuccessful Login Attempts	AC-7	AC-7	AC-7
AC-8	System Use Notification	AC-8	AC-8	AC-8
AC-9	Previous Logon Notification	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	Not Selected	Not Selected	AC-10
AC-11	Session Lock	Not Selected	AC-11	AC-11
AC-12	Session Termination	Not Selected	AC-12	AC-12 (1)
AC-13	Supervision and Review—Access Control	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Automated Marking	Not Selected	Not Selected	AC-15
AC-16	Automated Labeling	Not Selected	Not Selected	Not Selected

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)
AC-18	Wireless Access Restrictions	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Access Control for Portable and Mobile Devices	Not Selected	AC-19	AC-19
AC-20	Use of External Information Systems	AC-20	AC-20 (1)	AC-20 (1)
Awareness and Training				
AT-1	Security Awareness and Training Policy and Procedures	AT-1	AT-1	AT-1
AT-2	Security Awareness	AT-2	AT-2	AT-2
AT-3	Security Training	AT-3	AT-3	AT-3
AT-4	Security Training Records	AT-4	AT-4	AT-4
AT-5	Contacts with Security Groups and Associations	Not Selected	Not Selected	Not Selected
Audit and Accountability				
AU-1	Audit and Accountability Policy and Procedures	AU-1	AU-1	AU-1
AU-2	Auditable Events	AU-2	AU-2 (3)	AU-2 (1) (2) (3)
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1) (2)
AU-4	Audit Storage Capacity	AU-4	AU-4	AU-4
AU-5	Response to Audit Processing Failures	AU-5	AU-5	AU-5 (1) (2)
AU-6	Audit Monitoring, Analysis, and Reporting	Not Selected	AU-6 (2)	AU-6 (1) (2)
AU-7	Audit Reduction and Report Generation	Not Selected	AU-7 (1)	AU-7 (1)
AU-8	Time Stamps	AU-8	AU-8 (1)	AU-8 (1)
AU-9	Protection of Audit Information	AU-9	AU-9	AU-9
AU-10	Non-repudiation	Not Selected	Not Selected	Not Selected
AU-11	Audit Record Retention	AU-11	AU-11	AU-11
Certification, Accreditation, and Security Assessments				
CA-1	Certification, Accreditation, and Security Assessment Policies and Procedures	CA-1	CA-1	CA-1
CA-2	Security Assessments	CA-2	CA-2	CA-2
CA-3	Information System Connections	CA-3	CA-3	CA-3
CA-4	Security Certification	CA-4	CA-4 (1)	CA-4 (1)
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5
CA-6	Security Accreditation	CA-6	CA-6	CA-6
CA-7	Continuous Monitoring	CA-7	CA-7	CA-7
Configuration Management				
CM-1	Configuration Management Policy and Procedures	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	CM-2	CM-2 (1)	CM-2 (1) (2)
CM-3	Configuration Change Control	Not Selected	CM-3	CM-3 (1)
CM-4	Monitoring Configuration Changes	Not Selected	CM-4	CM-4
CM-5	Access Restrictions for Change	Not Selected	CM-5	CM-5 (1)

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
CM-6	Configuration Settings	CM-6	CM-6	CM-6 (1)
CM-7	Least Functionality	Not Selected	CM-7	CM-7 (1)
CM-8	Information System Component Inventory	CM-8	CM-8 (1)	CM-8 (1) (2)
Contingency Planning				
CP-1	Contingency Planning Policy and Procedures	CP-1	CP-1	CP-1
CP-2	Contingency Plan	CP-2	CP-2 (1)	CP-2 (1) (2)
CP-3	Contingency Training	Not Selected	CP-3	CP-3 (1)
CP-4	Contingency Plan Testing and Exercises	Not Selected	CP-4 (1)	CP-4 (1) (2)
CP-5	Contingency Plan Update	CP-5	CP-5	CP-5
CP-6	Alternate Storage Site	Not Selected	CP-6 (1) (3)	CP-6 (1) (2) (3)
CP-7	Alternate Processing Site	Not Selected	CP-7 (1) (2) (3)	CP-7 (1) (2) (3) (4)
CP-8	Telecommunications Services	Not Selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)
CP-9	Information System Backup	CP-9	CP-9 (1) (4)	CP-9 (1) (2) (3) (4)
CP-10	Information System Recovery and Reconstitution	CP-10	CP-10	CP-10 (1)
Identification and Authentication				
IA-1	Identification and Authentication Policy and Procedures	IA-1	IA-1	IA-1
IA-2	User Identification and Authentication	IA-2	IA-2 (1)	IA-2 (2) (3)
IA-3	Device Identification and Authentication	Not Selected	IA-3	IA-3
IA-4	Identifier Management	IA-4	IA-4	IA-4
IA-5	Authenticator Management	IA-5	IA-5	IA-5
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7
Incident Response				
IR-1	Incident Response Policy and Procedures	IR-1	IR-1	IR-1
IR-2	Incident Response Training	Not Selected	IR-2	IR-2 (1)
IR-3	Incident Response Testing and Exercises	Not Selected	IR-3	IR-3 (1)
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1)
IR-5	Incident Monitoring	Not Selected	IR-5	IR-5 (1)
IR-6	Incident Reporting	IR-6	IR-6 (1)	IR-6 (1)
IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)
Maintenance				
MA-1	System Maintenance Policy and Procedures	MA-1	MA-1	MA-1
MA-2	Controlled Maintenance	MA-2	MA-2 (1)	MA-2 (1) (2)
MA-3	Maintenance Tools	Not Selected	MA-3	MA-3 (1) (2) (3)
MA-4	Remote Maintenance	MA-4	MA-4 (1) (2)	MA-4 (1) (2) (3)
MA-5	Maintenance Personnel	MA-5	MA-5	MA-5

CNTL NO.	CONTROL NAME	CONTROL BASELINES		
		LOW	MOD	HIGH
MA-6	Timely Maintenance	Not Selected	MA-6	MA-6
Media Protection				
MP-1	Media Protection Policy and Procedures	MP-1	MP-1	MP-1
MP-2	Media Access	MP-2	MP-2 (1)	MP-2 (1)
MP-3	Media Labeling	Not Selected	Not Selected	MP-3
MP-4	Media Storage	Not Selected	MP-4	MP-4
MP-5	Media Transport	Not Selected	MP-5 (1) (2)	MP-5 (1) (2) (3)
MP-6	Media Sanitization and Disposal	MP-6	MP-6	MP-6 (1) (2)
Physical and Environmental Protection				
PE-1	Physical and Environmental Protection Policy and Procedures	PE-1	PE-1	PE-1
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2
PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)
PE-4	Access Control for Transmission Medium	Not Selected	Not Selected	PE-4
PE-5	Access Control for Display Medium	Not Selected	PE-5	PE-5
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (2)
PE-7	Visitor Control	PE-7	PE-7 (1)	PE-7 (1)
PE-8	Access Records	PE-8	PE-8	PE-8 (1) (2)
PE-9	Power Equipment and Power Cabling	Not Selected	PE-9	PE-9
PE-10	Emergency Shutoff	Not Selected	PE-10	PE-10 (1)
PE-11	Emergency Power	Not Selected	PE-11	PE-11 (1)
PE-12	Emergency Lighting	PE-12	PE-12	PE-12
PE-13	Fire Protection	PE-13	PE-13 (1) (2) (3)	PE-13 (1) (2) (3)
PE-14	Temperature and Humidity Controls	PE-14	PE-14	PE-14
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)
PE-16	Delivery and Removal	PE-16	PE-16	PE-16
PE-17	Alternate Work Site	Not Selected	PE-17	PE-17
PE-18	Location of Information System Components	Not Selected	PE-18	PE-18 (1)
PE-19	Information Leakage	Not Selected	Not Selected	Not Selected
Planning				
PL-1	Security Planning Policy and Procedures	PL-1	PL-1	PL-1
PL-2	System Security Plan	PL-2	PL-2	PL-2
PL-3	System Security Plan Update	PL-3	PL-3	PL-3
PL-4	Rules of Behavior	PL-4	PL-4	PL-4
PL-5	Privacy Impact Assessment	PL-5	PL-5	PL-5
PL-6	Security-Related Activity Planning	Not Selected	PL-6	PL-6

Personnel Security				
PS-1	Personnel Security Policy and Procedures	PS-1	PS-1	PS-1
PS-2	Position Categorization	PS-2	PS-2	PS-2
PS-3	Personnel Screening	PS-3	PS-3	PS-3
PS-4	Personnel Termination	PS-4	PS-4	PS-4
PS-5	Personnel Transfer	PS-5	PS-5	PS-5
PS-6	Access Agreements	PS-6	PS-6	PS-6
PS-7	Third-Party Personnel Security	PS-7	PS-7	PS-7
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8
Risk Assessment				
RA-1	Risk Assessment Policy and Procedures	RA-1	RA-1	RA-1
RA-2	Security Categorization	RA-2	RA-2	RA-2
RA-3	Risk Assessment	RA-3	RA-3	RA-3
RA-4	Risk Assessment Update	RA-4	RA-4	RA-4
RA-5	Vulnerability Scanning	Not Selected	RA-5	RA-5 (1) (2)
System and Services Acquisition				
SA-1	System and Services Acquisition Policy and Procedures	SA-1	SA-1	SA-1
SA-2	Allocation of Resources	SA-2	SA-2	SA-2
SA-3	Life Cycle Support	SA-3	SA-3	SA-3
SA-4	Acquisitions	SA-4	SA-4 (1)	SA-4 (1)
SA-5	Information System Documentation	SA-5	SA-5 (1)	SA-5 (1) (2)
SA-6	Software Usage Restrictions	SA-6	SA-6	SA-6
SA-7	User Installed Software	SA-7	SA-7	SA-7
SA-8	Security Engineering Principles	Not Selected	SA-8	SA-8
SA-9	External Information System Services	SA-9	SA-9	SA-9
SA-10	Developer Configuration Management	Not Selected	Not Selected	SA-10
SA-11	Developer Security Testing	Not Selected	SA-11	SA-11
System and Communications Protection				
SC-1	System and Communications Protection Policy and Procedures	SC-1	SC-1	SC-1
SC-2	Application Partitioning	Not Selected	SC-2	SC-2
SC-3	Security Function Isolation	Not Selected	Not Selected	SC-3
SC-4	Information Remnance	Not Selected	SC-4	SC-4
SC-5	Denial of Service Protection	SC-5	SC-5	SC-5
SC-6	Resource Priority	Not Selected	Not Selected	Not Selected
SC-7	Boundary Protection	SC-7	SC-7 (1) (2) (3) (4) (5)	SC-7 (1) (2) (3) (4) (5) (6)
SC-8	Transmission Integrity	Not Selected	SC-8	SC-8 (1)
SC-9	Transmission Confidentiality	Not Selected	SC-9	SC-9 (1)
SC-10	Network Disconnect	Not Selected	SC-10	SC-10
SC-11	Trusted Path	Not Selected	Not Selected	Not Selected

SC-12	Cryptographic Key Establishment and Management	Not Selected	SC-12	SC-12
SC-13	Use of Cryptography	SC-13	SC-13	SC-13
SC-14	Public Access Protections	SC-14	SC-14	SC-14
SC-15	Collaborative Computing	Not Selected	SC-15	SC-15
SC-16	Transmission of Security Parameters	Not Selected	Not Selected	Not Selected
SC-17	Public Key Infrastructure Certificates	Not Selected	SC-17	SC-17
SC-18	Mobile Code	Not Selected	SC-18	SC-18
SC-19	Voice Over Internet Protocol	Not Selected	SC-19	SC-19
SC-20	Secure Name /Address Resolution Service (Authoritative Source)	Not Selected	SC-20	SC-20
SC-21	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	Not Selected	Not Selected	SC-21
SC-22	Architecture and Provisioning for Name/Address Resolution Service	Not Selected	SC-22	SC-22
SC-23	Session Authenticity	Not Selected	SC-23	SC-23
System and Information Integrity				
SI-1	System and Information Integrity Policy and Procedures	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring Tools and Techniques	Not Selected	SI-4 (4)	SI-4 (2) (4) (5)
SI-5	Security Alerts and Advisories	SI-5	SI-5	SI-5 (1)
SI-6	Security Functionality Verification	Not Selected	Not Selected	SI-6
SI-7	Software and Information Integrity	Not Selected	Not Selected	SI-7 (1) (2)
SI-8	Spam Protection	Not Selected	SI-8	SI-8 (1)
SI-9	Information Input Restrictions	Not Selected	SI-9	SI-9
SI-10	Information Accuracy, Completeness, Validity, and Authenticity	Not Selected	SI-10	SI-10
SI-11	Error Handling	Not Selected	SI-11	SI-11
SI-12	Information Output Handling and Retention	Not Selected	SI-12	SI-12