CGI

Experience the commitment®

Developing a Framework to Improve Critical Infrastructure Cybersecurity

A Global IT Partner Perspective

Response to National Institute of Standards and Technology (NIST) [Docket Number 130208119–3119–01] Request for Information

CGI RESPONSE TO NIST’S REQUEST FOR INFORMATION

With 71,000 professionals operating in 400 offices and 40 countries, CGI provides business consulting, systems integration and outsourcing services to private and public sector clients across the globe. As such, we provide NIST with an additional industry perspective – that of an information technology and cybersecurity partner supporting critical infrastructure sector companies, both large and small, as well as the federal, state, local, tribal, and municipal public sector entities.

UNDERSTANDING: THE CURRENT CRITICAL INFRASTRUCTURE CYBERSECURITY LANDSCAPE

Focus on the safety and security of the U.S. critical infrastructure has increased in the wake of cyber attacks and intrusions targeting a breadth of industries (from energy to transportation, financial services to technology). On February 12, 2013, the U.S. Executive branch issued Executive Order (EO) 13636,"Improving Critical Infrastructure Cybersecurity" and Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience," calling for increased attention, coordination, cooperation, and action to secure the nation's critical infrastructure. In these documents, the Executive Branch articulated the complexity associated with the protecting the nation's critical infrastructure – the breadth of systems and assets across the broad spectrum of sectors within the "critical infrastructure" definition. The Order and Directive detail 16 discrete sectors that encompass the nation's critical infrastructure:

- Chemical
- Commercial facilities
- Communications
- Critical manufacturing
- Dams
- Defense industrial
- Emergency services
- Energy
- Financial services
- Food and agriculture
- Government facilities
- Health
- IT
- Nuclear
- Transportation
- Water

These significant documents further articulated the roles that organizations and agencies within the federal government will take in working with critical infrastructure owners and operators, as well as with state, local, tribal, and territorial entities, in proactively mitigating risk and strengthening the security posture of the nation's critical infrastructure.

DEFINING "CRITICAL INFRASTRUCTURE"

The Executive Order and Presidential Policy Directive define critical infrastructure as:

> *"[S]ytems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."*

NIST'S ROLE: ESTABLISHING THE CYBERSECURITY FRAMEWORK

As the nation moves forward in putting the programs described in the EO and PPD into action, NIST will play a critical role in establishing the Cybersecurity Framework that will underpin the Cybersecurity Program. Building upon existing standards and industry best practices, the Cybersecurity Framework will include "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks." Upon publication of the Framework, to be accomplished no later than February 12, 2014, regulatory agencies will propose the means by which the standards and best practices articulated within the Framework should be put into action.

Through this Request for Information process and a series of ongoing workshops, NIST provides impacted industries and public sector entities the ability to contribute to the significant conversation surrounding the objectives of Framework development. NIST's efforts will include cross-sector security standards and guidelines as well as areas for improvement in cybersecurity in collaboration with particular sectors and/or standards-developing organizations relevant to one or more sectors.

The government recognizes the impact that the new Framework and focus on critical infrastructure cybersecurity will have on both the private sector and the public sector, including the potential for new regulations, new voluntary programs, requirements for cyber risk information sharing, and implications related to liability, civil liberties, and industries' bottom line.

ABOUT CGI

The world's 5th largest independent IT and business process services firm, with annualized revenue exceeding $10 billion, CGI' supports the business needs of our public and private sector clients around the globe. CGI offers its end-to-end services to a selected set of economic sectors covering 90% of global IT spend, encompassing each of the critical infrastructure sectors defined by the Executive Order and the Presidential Policy Directive.

- **Financial services** – Helping financial institutions, including most major banks and top insurers, reduce cost and risk, increase efficiency, and improve customer service.
- **Health** – Helping more than 1,000 healthcare facilities, hospitals and departments of health implement solutions for better care, better business and better outcomes.
- **Communications** – Helping six of the top 10 global telecom providers deliver broad telecommunications services, new technology solutions that improve and expand communications capabilities, and improved productivity and service.
- **Energy** – Supporting three of the top six oil companies and a host of utility companies, both large and small, in improving quality and security of critical energy resources.
- **Critical manufacturing** – Enabling business operations and transformation for more than 2,000 manufacturing, retail, and distribution clients.
- **Government** – Supporting over 2,000 global government organizations in reducing costs and improving the efficiency, quality and accountability of public services. In the U.S., CGI directly supports the efforts of all three branches of the U.S. federal government and each of the government agencies identified as sector-specific agencies (SSAs) in the Presidential Policy Directive, including the Department of Homeland Security, the Department of Defense, the General Services Administration, the U.S. Environmental Protection Agency, the Department of Transportation, the Department of Energy, the Department of Health and Human Services, and the U.S. Department of Agriculture.

As a global IT leader, CGI pays close attention to cyber attacks and risks associated with our own data centers and IT assets as well as the assets of the customers we serve. To support our government and industry partners, CGI provides end-to-end security offerings to include:

- **Enterprise security management** – includes the governance, strategies, frameworks, plans and assessments necessary to create and manage an effective enterprise-wide security program
- **Security engineering** – encompasses the architecture, design, development and deployment of solutions and services that secure your information assets and infrastructure
- **Business continuity** – ensures that the contingency plans and enablers are in place to keep your business running when disaster hits
- **Managed security services** – provides reliable protection from viruses, hacker intrusions, spam and other unwanted Internet traffic to guard your enterprise from downtime and other productivity losses
- **Cloud security** – provides confidence that clients' data is protected in a cloud computing environment
- **Industrial Control Systems cybersecurity** – methodologies, frameworks, products, and services for cyber security in Industrial Control Systems (ICS) environments based on a risk assessment approach for industrial process automation and control systems environments
- **Federal cybersecurity** – products and services that help U.S. federal agencies protect themselves from ever-evolving cyber attacks, to include advanced analytics, computer network defense, and federal identity management solutions

> *Cybersecurity is "one of the top issues out there for governments and industry. There are no boundaries when it comes to cyber warfare. It crosses boundaries. There's no geographic block here when it comes to this kind of an attack."*
>
> **Michael Roach,** President and CEO of CGI Group, during interview by Business News Network on March 13, 2013

Our federal IT security practice leverages investments in security innovation and expertise—such as our Cyber Global Innovations Lab—that accelerate new technology and tactics from research to test to operations. CGI's cyber view spans the globe, with direct support for large critical infrastructures with national and global implications.

WATER

Large water companies across the globe trust CGI with enhancing their security posture through advanced, integrated approaches. Welsh Water, responsible for distribution of drinking water to homes across Wales, contracted with CGI to support contingency and disaster planning for continuity of services in case of catastrophic event. In Australia, CGI implemented DNP3 Secure Authentication for remote outstations. Sydney Water Corporation looked to CGI to upgrade its security architecture to address the differing priorities, design parameters, and implementation considerations associated with its corporate network, external-facing information systems, and plant SCADA systems.

ELECTRICAL/POWER

CGI is responsible for systems running 10 out of 16 of the world's energy markets. We are partner to more than 200 energy clients worldwide, including global and U.S.-based utilities such as EON, Hydro-Québec, EDF, Tacoma Power, Southern California Edison, GDFSuez, EDP, RWE, Hydro One, Exelon Energy Delivery, Baltimore Gas & Electric, Idaho Power, Public Service Electric and Gas, and Oklahoma Gas and Electric. CGI supports Portugal's InovGrid project, automating grid management using CGI's Instant Energy platform, with a keen focus on securing the automated grid. CGI's PragmaLINE, used by Tacoma Power, analyzes operating data to help predict and monitor potential distribution network failures. Global renewable energy firm EDP partners with CGI for its SCADA security architecture, instilling confidence that EDP "can protect ourselves effectively from the cyber security threats."[1] For the nuclear industry, CGI has also developed workflow and document management solutions for gathering of evidence and control of regulatory processes to help Nuclear facilities avoid non-compliance penalties.

PETROLEUM

CGI supports three of the world's top oil companies. Our Process Control Device (PCD) Security Service offers a suite of services around the physical and network security of the critical infrastructure (process control environments) for Oil and Gas Refining and Exploration businesses. We serve as a global partner of Shell Oil, one of the globe's top three oil and gas companies, providing application managed services, shared services, project and consultancy services, and advanced security services for sub-surface and wells, refineries, and offshore and onshore exploration facilities. In fact, based upon the success of the simultaneous cybersecurity initiatives at this corporation's 27 oil refineries – including physical security, network upgrades, asset hardening, and cyber intrusion monitoring – CGI has been engaged to execute additional upstream cybersecurity initiatives at offshore and onshore exploration facilities.

HEALTHCARE

Hospital and health insurers leverage CGI solutions and services to support critical health IT initiatives. CGI's RFID "track and trace" solutions assist pharmaceuticals firms to authenticate, monitor and control the flow of drugs through the channel, helping to control loss and counterfeiting. The Department of Health and Human Services trusted CGI with architecting the federal health insurance exchange, and numerous states have also looked to CGI to build and host their statewide health insurance exchange (HIX) programs.

[1] Aurelio Blanquet, Director of Automation, Telecontrol and Telecommunications at EDP

CRITICAL MANUFACTURING AND SUPPLY CHAIN

CGI's provides IT services for multiple manufacturing segments, including aerospace, mining & metals, automotive and consumer packaged goods including clients such as IT Alstom, Bombardier, Rio Tinto Alcan, Michelin and Philips International. CGI's Logica division's Intelligent Freight and Transportation (LIFT) solution provides advanced, real-time information about the exact location and status of goods within the supply chain to optimize security for goods transported by land, air or sea. CGI is the partner of global life and materials sciences firm Royal DSM, implementing and optimizing cybersecurity in their manufacturing and process automation / plant domains.

FINANCIAL SERVICES

CGI's Intellectual Property is used across the banking, finance, and insurance sectors. Our federal financial management platform, Momentum, is used by 40,000 users, with 25,000 users of our Momentum timekeeping system. CGI's solutions facilitate core federal agency financial transactions including general ledger management, funds management, payment management, receivable management, cost management and external reporting. CGI case management, claims processing, and insurance underwriting solutions underpin the secure business transactions of global insurance firms such as are used by global banking and insurance firms such as Manulife, John Hancock, the Hartford, Chubb, Forester, Desjardins, FirstAssist, and Commerce Insurance.

DEFENSE

CGI's 80-person team provides network security services and supports the Computer Network Defense (CND) and Information Assurance (IA) Enterprise Security organizations protecting the Pentagon. CGI provides primary support for PENTCIRT Incident Handling Operations for the Capital Area Region. We continuously monitor 100K unclassified systems/nodes, along with an undisclosed number of classified systems/nodes, with an estimated 50M events per day. In addition, as systems integrator for DISA's DoD enterprise-wide Web Content Filtering program, CGI continuously monitors 166 enterprise-level devices across 10 enterprise-level systems to capture and analyze an average of 2 billion events per day. We perform similar cyber support functions across the globe, such as in the United Kingdom, where CGI directly interacts with Critical Protection of the National Infrastructure (CPNI) as an information supplier and recipient of early alert notifications.

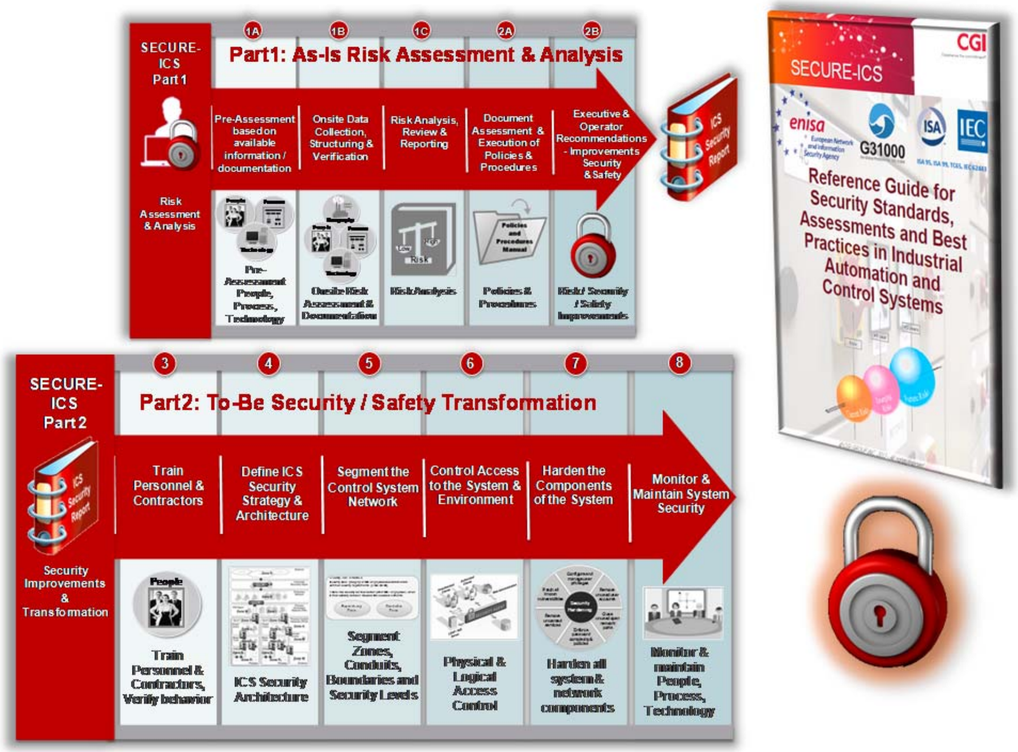
CGI Response to NIST RFI Questions/Requests for Comment

In the following sections, we address a number of the questions posted in the NIST RFI, focusing on those areas where CGI's experience may provide NIST the most value in considering the planned Framework effort.

The answers that CGI provide on the questions in this RFI are based on CGI's own corporate experience and our experience and expertise as a consulting firm providing cybersecurity services for in several industry sectors. CGI's focus is directly on Information Technology (IT) and Industrial Control Systems (ICS) environments. CGI has developed a sector-independent Cyber Security Management Framework (CSMF) as well as a cybersecurity approach for industrial environments (SECURE-ICS) – both of which are relevant to NIST's Framework initiative. The foundation of CGI's CSMF are SECURE-ICS is based on the results of the USA Chemical Sector Cyber Security Program and the presented cybersecurity management system (CSMS); the ISA99, Industrial Automation and Control Systems Security (ISA 99), and IEC 62443 enterprise control system integration standards.

From an IT perspective, we are further guided by ISO 27002/17799 and NIST (e.g., 800-14 and 800-26 as well as 800-37 and 800-53 related to our federal agency data and application hosting) as well as other security best practices and international standards.

For multiple critical infrastructure sectors we support from an IT and security consulting perspective – including but not limited to chemical, communications, energy, transportation, utilities, and water – CGI has enhanced the CSMF and the SECURE-ICS framework and approach with ICS specific network and data protection policies as well as with baseline requirements for SCADA and embedded devices like programmable logic controls (PLCs) and baselines for ICS servers, laptops, desktops, file hosting and webhosting.


SECURE-ICS Part 1
Risk Assessment & Analysis
1A
1B
1C
2A
2B
Part1: As-Is Risk Assessment & Analysis
Pre-Assessment based on available information / documentation
Onsite Data Collection, Structuring & Verification
Risk Analysis, Review & Reporting
Document Assessment & Execution of Policies & Procedures
Executive & Operator Recommendations - Improvements Security & Safety
Pre-Assessment People, Process, Technology
Onsite Risk Assessment & Documentation
Risk Analysis
Policies & Procedures
Risk / Security / Safety Improvements
ICS Security Report
SECURE-ICS Part 2
Security Improvements & Transformation
3
4
5
6
7
8
Part2: To-Be Security / Safety Transformation
Train Personnel & Contractors
Define ICS Security Strategy & Architecture
Segment the Control System Network
Control Access to the System & Environment
Harden the Components of the System
Monitor & Maintain System Security
Train Personnel & Contractors, Verify behavior
ICS Security Architecture
Segment Zones, Conduits, Boundaries and Security Levels
Physical & Logical Access Control
Harden all system & network components
Monitor & maintain People, Process, Technology
CGI
SECURE-ICS
enisa
G31000
ISA
IEC
Reference Guide for Security Standards, Assessments and Best Practices in Industrial Automation and Control Systems

Current Risk Management Practices

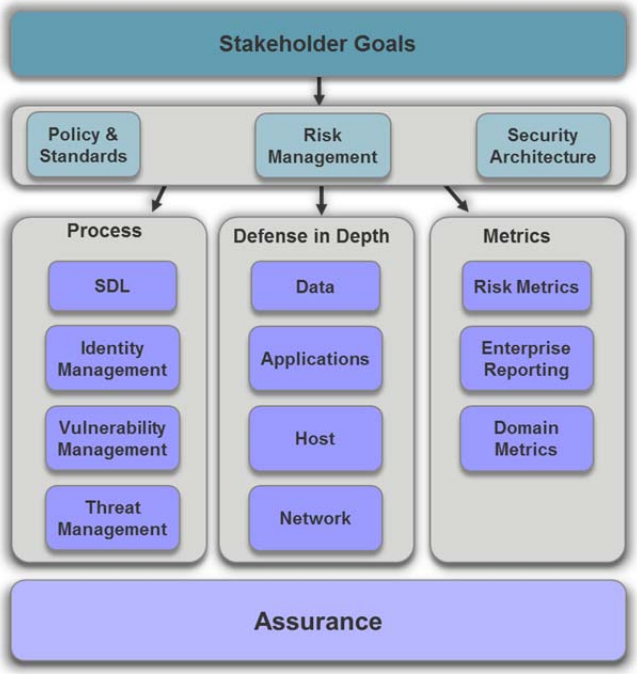
WHAT DO ORGANIZATIONS SEE AS THE GREATEST CHALLENGES IN IMPROVING CYBERSECURITY PRACTICES ACROSS CRITICAL INFRASTRUCTURE?

Industries within the critical infrastructure sectors provide the essentials of modern life and defend our national security; their services impact national economic security, national public health and safety. Many sector components influence or impact any combination of these critical national concerns. Cybersecurity is an integral part of overall critical infrastructure sectors security and the industry is addressing the risk as a sector-wide initiative, to minimize the potential impact to both public safety and the economy.

Because the sectors touch so many aspects of how we live our lives and how business is conducted throughout the world, **technology, connectivity and information exchange** are three of the greatest challenges and essential aspects of company operations and processes in the sectors. However, the same technologies that make business operations and critical infrastructure processes more efficient can introduce new vulnerabilities. As the world faces increased threats, the critical infrastructure sectors needs to increase its capability to manage exposure to cybersecurity risk and protect against the threat of unauthorized access to information being used to facilitate or cause a physical attack or disruption in the supply chain.

Reducing current and future cybersecurity risks requires a combination of leading-edge technology, accepted sector practices, and timely information sharing throughout and across sectors. Sector-wide cooperation and cross-collaboration to address cybersecurity issues has many precedents.

Key in the critical infrastructure environment is adoption of a cybersecurity architecture, principles and guidelines as described in the ISA 99 and IEC 62443 standards. The architecture must separate each of the five security zones for each different type of technology/machine within these critical infrastructures while addressing the well-defined conduits between these zones. Based upon that concept, additional procedures relative to people, processes, and technologies can be defined to complete the overall view of cybersecurity for both ICS and across the enterprise.



The cybersecurity architecture must be based upon a mature risk, threats, and vulnerabilities assessment. The challenge for industries of all sizes and across all sectors is the need to be pragmatic within known restrictions (e.g., budget, access to expertise, multi-national considerations). The approaches borne from the risk assessment and defined cybersecurity architecture must be not only implemented, but continually assessed and monitored over time.

WHAT DO ORGANIZATIONS SEE AS THE GREATEST CHALLENGES IN DEVELOPING A CROSS-SECTOR STANDARDS-BASED FRAMEWORK FOR CRITICAL INFRASTRUCTURE?

As NIST looks to address sectors and organization’s challenges through a cross-sector, standards-based framework, it must consider the significant challenge of providing information and guidance to assist organizations in implementing a cybersecurity management framework and appropriate controls. A cybersecurity management framework, such as the framework adopted by CGI, is meant to stimulate thinking and provide resources that a company can use as it determines its approach to implementing corporate security management practices across its information systems, critical infrastructure, and process control systems. These cybersecurity activities must be integrated within the organization’s enterprise-wide security program and aligned with the organization’s value networks. The cybersecurity activities should be integrated into an organization’s security program, aligned with organizations in the value networks.

Some organizations are challenged in how to begin to discuss and document a framework. The framework structure must be consistent for each of the cybersecurity management framework elements. For each element, the following sections must be provided: introduction, statement of management practices, applicability to the industry / critical infrastructure sector, general baseline practices, how organization are approaching the topic, and a list of the resources used to support the topic.

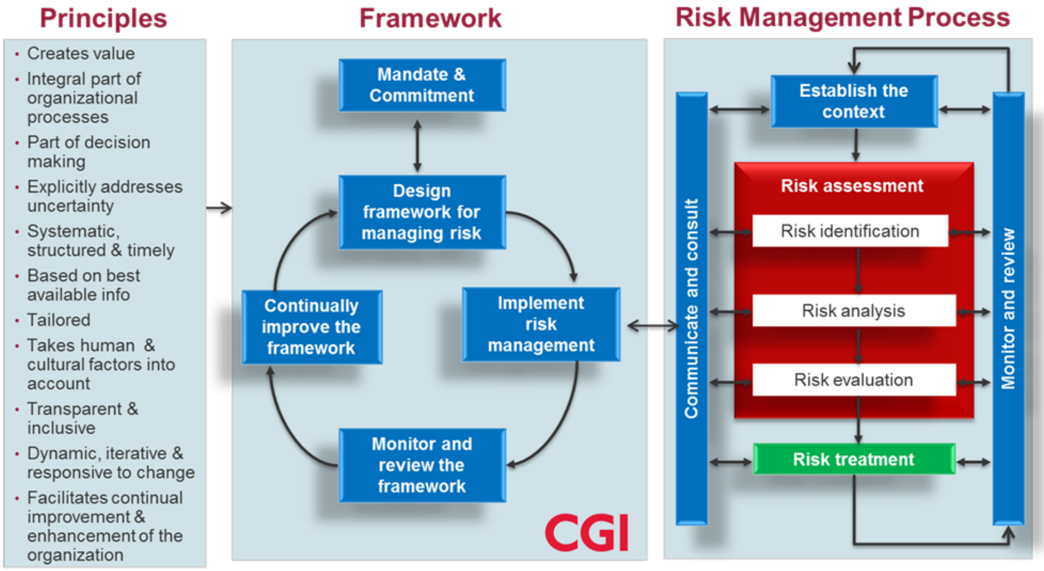
These elements cover various activities that are frequently included in efforts to comprehensively manage cybersecurity. Management frameworks require that policies, procedures and guidelines be developed, roles and responsibilities assigned, and resources allocated. The heart of a management framework is the Deming Plan-Do-Check-Act (PDCA) cycle.

DESCRIBE YOUR ORGANIZATION'S POLICIES AND PROCEDURES GOVERNING RISK GENERALLY AND CYBERSECURITY RISK SPECIFICALLY. HOW DOES SENIOR MANAGEMENT COMMUNICATE AND OVERSEE THESE POLICIES AND PROCEDURES?

As a large, global company with significant revenue and reach, CGI has a baseline set of cybersecurity policies and procedures for IT and ICS as well as a methodology for risk assessment. We have resources with expertise in implementing the policies and procedures defined in our CSMF as well as the ability and responsibility to inform and educate our global resources on those policies, procedures, and techniques.

While most organization resources may think first of security policies as they relate to physical security (e.g., building access) and IT security (e.g., rules for information security, password protection, and data retention), the CSMF must also addresses process control systems. It is important to note that traditionally, process control systems were designed with the purposes of control and safety in mind. Such systems previously communicated most frequently via LAN and leveraged proprietary standards. However, more recently, these systems are increasingly networked and often accessible via internet, increasing their vulnerability to attack. Systems, therefore, designed with little cybersecurity considerations in mind are now exposed to threats they were never expected to encounter, such as worms, viruses and hackers.

There are potentially serious consequences should these vulnerabilities be exploited. The impacts of an electronic attack on process control systems can include, for example: denial of service, unauthorized control of the process, loss of integrity, loss of confidentiality, loss of reputation and health, safety and environmental impacts. For CGI, risk management is addressed by using a SCADA / ICS Risk Management Framework based on the ISO 31000 standards.


Principles
Creates value
Integral part of organizational processes
Part of decision making
Explicitly addresses uncertainty
Systematic, structured & timely
Based on best available info
Tailored
Takes human & cultural factors into account
Transparent & inclusive
Dynamic, iterative & responsive to change
Facilitates continual improvement & enhancement of the organization
Framework
Mandate & Commitment
Design framework for managing risk
Implement risk management
Monitor and review the framework
Continually improve the framework
CGI
Risk Management Process
Establish the context
Risk assessment
Risk identification
Risk analysis
Risk evaluation
Risk treatment
Communicate and consult
Monitor and review

Senior management is involved and responsible for validating and communicating these policies and procedures, while the corporate cybersecurity team leads assessment, implementing, and control of policies and requirements. For those organizations with SCADA systems, the corporate cybersecurity team is typically charged with supporting the operational plant managers and operators in assessing, implementing and controlling the policies and requirements.

WHERE DO ORGANIZATIONS LOCATE THEIR CYBERSECURITY RISK MANAGEMENT PROGRAM/OFFICE?

Cybersecurity and risk management are primarily organized in a federated structure. On corporate level, the cybersecurity team or unit is responsible for defining the security policies, guidelines and requirements as well as for doing risk assessments at corporate level. In plants or process automation domains, the plant manager is responsible for the cybersecurity assessment at plant level, supported by the corporate organization.

Therefore it is necessary to have pragmatic cybersecurity policies, documented requirements, and guidelines for dealing with the assessed risk and level of protection/risk that is acceptable for a given plant/facility and for the enterprise. These may be the same across locations/facilities or different depending upon a number of variables (articulated through the risk assessment process). With plant decentralization, organizations must also determine whether the approach to a risk at Location A warrants the same or a varied approach at Location B.

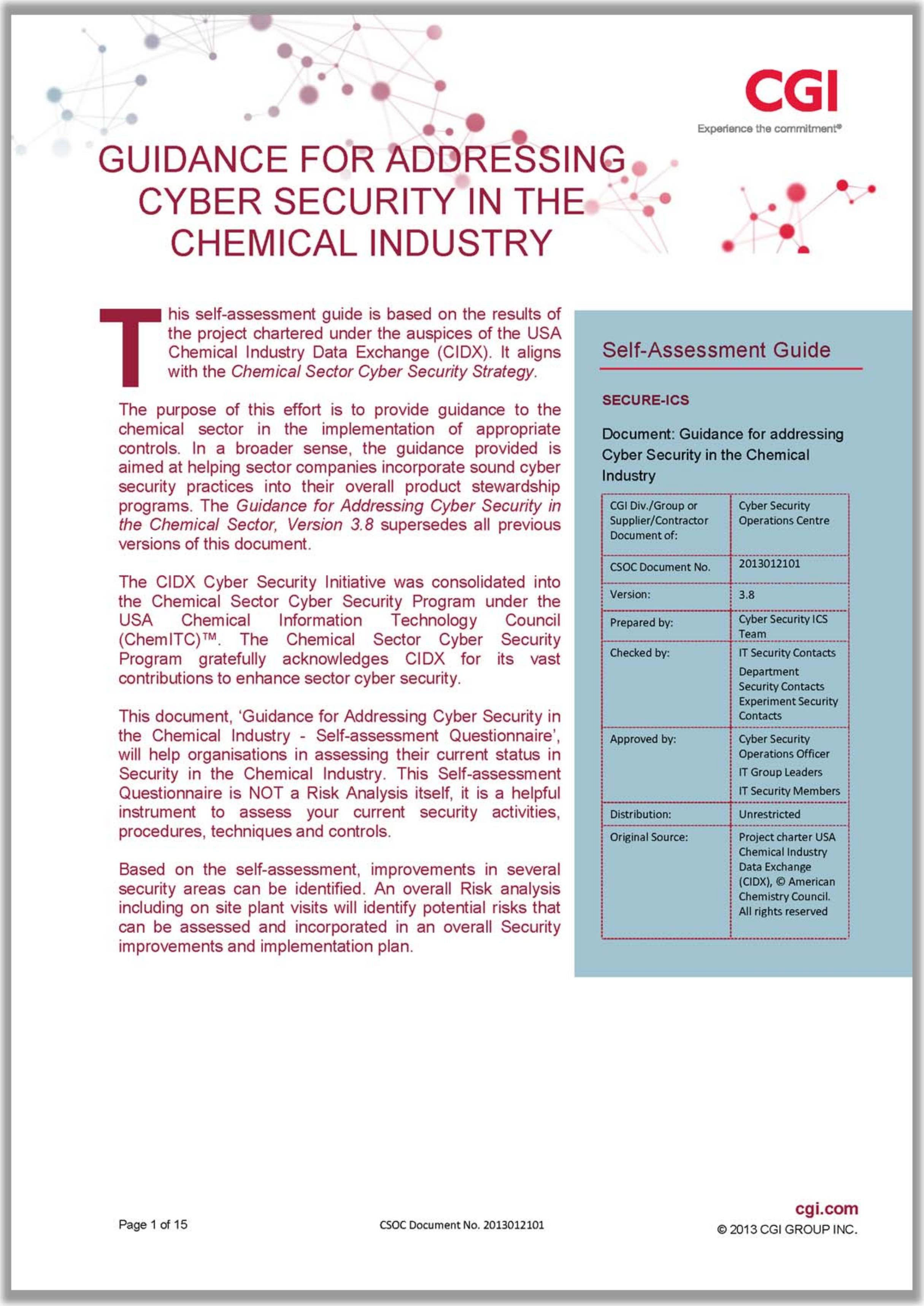
HOW DO ORGANIZATIONS DEFINE AND ASSESS RISK GENERALLY AND CYBERSECURITY RISK SPECIFICALLY?

Within CGI's approach, risk management – specifically risk management as it pertains to SCADA/ICS within the overall risk management framework – is based on the ISO 31000 standards, as depicted on page 7 of this response. Based on the concepts of this risk management framework, we use a set of ICS Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines that will cover the risk identification part of the framework. These audit guidelines will help the cybersecurity team in assessing the different areas of the plant environment. These critical controls encompass 20 core areas:

- Inventory of Authorized and Unauthorized Devices
- Inventory of Authorized and Unauthorized Software
- Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
- Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
- Boundary Defense
- Maintenance, Monitoring, and Analysis of Audit Logs
- Application Software Security
- Controlled Use of Administrative Privileges
- Controlled Access Based on Need to Know
- Continuous Vulnerability Assessment and Remediation
- Account Monitoring and Control
- Malware Defenses
- Limitation and Control of Network Ports, Protocols, and Services
- Wireless Device Control
- Data Loss Prevention
- Secure Network Engineering

- Penetration Tests and Red Team Exercises
- Incident Response Capability
- Data Recovery Capability
- Security Skills Assessment and Appropriate Training to Fill Gaps

Self-assessment is a critical tool at the facility/plant level. Where plant managers and operators require guidance and assistance in identifying the plant risks at the various security levels, CGI has developed a Risk (Self) Assessment Guide to support our clients in such endeavors. On the following pages, we provide an overview of one such Risk (Self) Assessment Guide, created specifically to meet the needs of CGI's customer base within the Chemical Industry. The information to follow on pages 10-12 of this response are taken from CGI's "Guidance for Addressing Cyber Security in the Chemical Industry," version 3.8.



CGI

Experience the commitment®

GUIDANCE FOR ADDRESSING CYBER SECURITY IN THE CHEMICAL INDUSTRY

This self-assessment guide is based on the results of the project chartered under the auspices of the USA Chemical Industry Data Exchange (CIDX). It aligns with the *Chemical Sector Cyber Security Strategy*.

The purpose of this effort is to provide guidance to the chemical sector in the implementation of appropriate controls. In a broader sense, the guidance provided is aimed at helping sector companies incorporate sound cyber security practices into their overall product stewardship programs. The *Guidance for Addressing Cyber Security in the Chemical Sector, Version 3.8* supersedes all previous versions of this document.

The CIDX Cyber Security Initiative was consolidated into the Chemical Sector Cyber Security Program under the USA Chemical Information Technology Council (ChemITC)™. The Chemical Sector Cyber Security Program gratefully acknowledges CIDX for its vast contributions to enhance sector cyber security.

This document, 'Guidance for Addressing Cyber Security in the Chemical Industry - Self-assessment Questionnaire', will help organisations in assessing their current status in Security in the Chemical Industry. This Self-assessment Questionnaire is NOT a Risk Analysis itself, it is a helpful instrument to assess your current security activities, procedures, techniques and controls.

Based on the self-assessment, improvements in several security areas can be identified. An overall Risk analysis including on site plant visits will identify potential risks that can be assessed and incorporated in an overall Security improvements and implementation plan.

Self-Assessment Guide

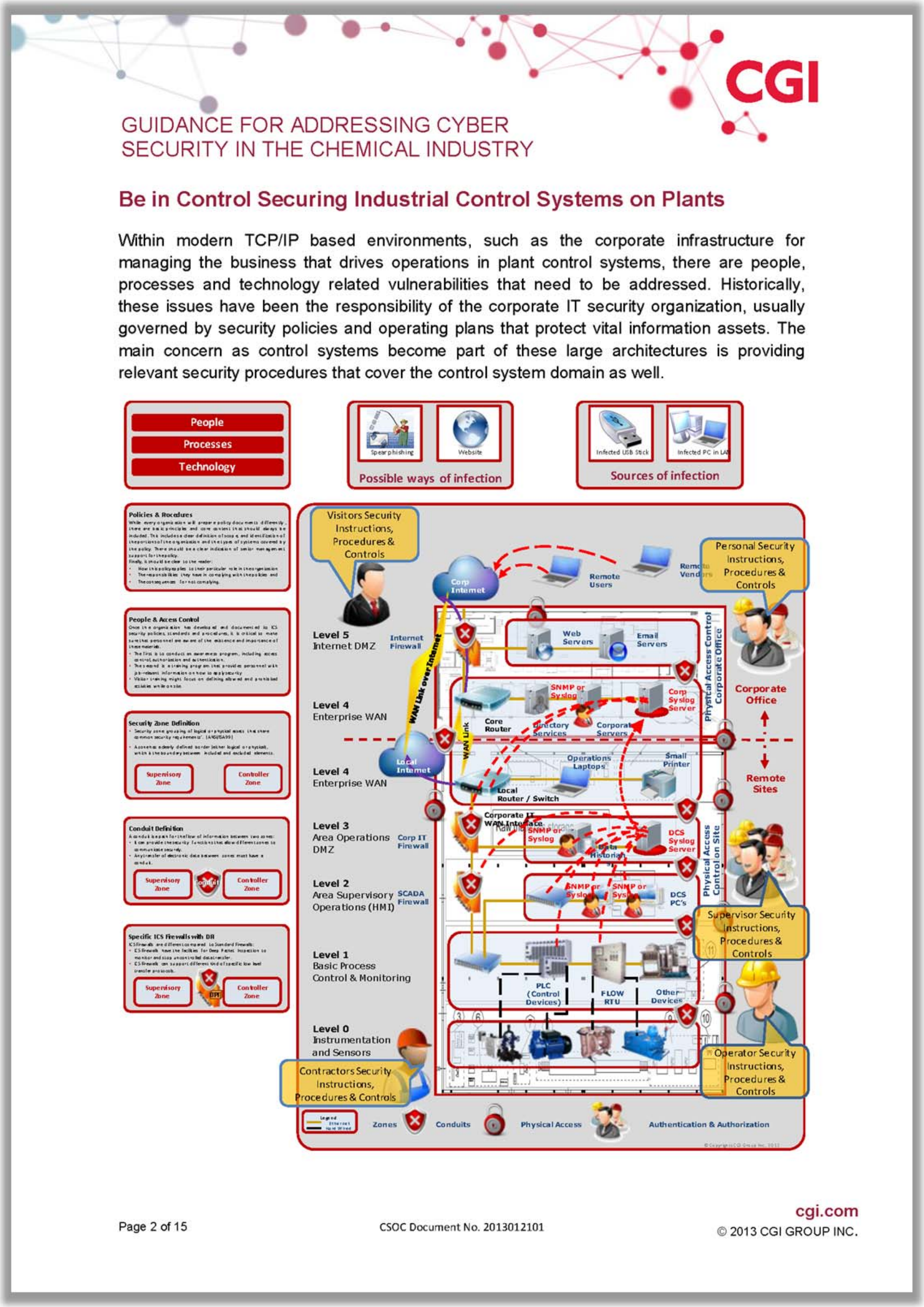
SECURE-ICS

Document: Guidance for addressing Cyber Security in the Chemical Industry

CGI Div./Group or Supplier/Contractor Document of:	Cyber Security Operations Centre
CSOC Document No.	2013012101
Version:	3.8
Prepared by:	Cyber Security ICS Team
Checked by:	IT Security Contacts Department Security Contacts Experiment Security Contacts
Approved by:	Cyber Security Operations Officer IT Group Leaders IT Security Members
Distribution:	Unrestricted
Original Source:	Project charter USA Chemical Industry Data Exchange (CIDX), © American Chemistry Council. All rights reserved

Page 1 of 15 CSOC Document No. 2013012101

cgi.com



GUIDANCE FOR ADDRESSING CYBER SECURITY IN THE CHEMICAL INDUSTRY

Be in Control Securing Industrial Control Systems on Plants

Within modern TCP/IP based environments, such as the corporate infrastructure for managing the business that drives operations in plant control systems, there are people, processes and technology related vulnerabilities that need to be addressed. Historically, these issues have been the responsibility of the corporate IT security organization, usually governed by security policies and operating plans that protect vital information assets. The main concern as control systems become part of these large architectures is providing relevant security procedures that cover the control system domain as well.

Policies & Rocedures

While every organization will prepare policy documents differently, there are basic principles and core content that should always be included. This includes a clear definition of scope, and identification of the portions of the organization and the types of systems covered by the policy. There should be a clear indication of senior management support for the policy.
Finally, it should be clear to the reader:

- How this policy applies to their particular role in the organization
- The responsibilities they have in complying with the policies and
- The consequences for not complying.

People & Access Control

Once the organization has developed and documented its ICS security policies, standards and procedures, it is critical to make sure that personnel are aware of the existence and importance of these materials.

- The first is to conduct an awareness program, including access control, authorization and authentication.
- The second is a training program that provides personnel with job-relevant information on how to apply security.
- Visitor training might focus on defining allowed and prohibited activities while on site.

Security Zone Definition

- Security zone: grouping of logical or physical assets that share common security requirements". (ANSI/ISA99)
- A zone has a clearly defined border (either logical or physical), which is the boundary between included and excluded elements.

Conduit Definition

A conduit is a path for the flow of information between two zones:

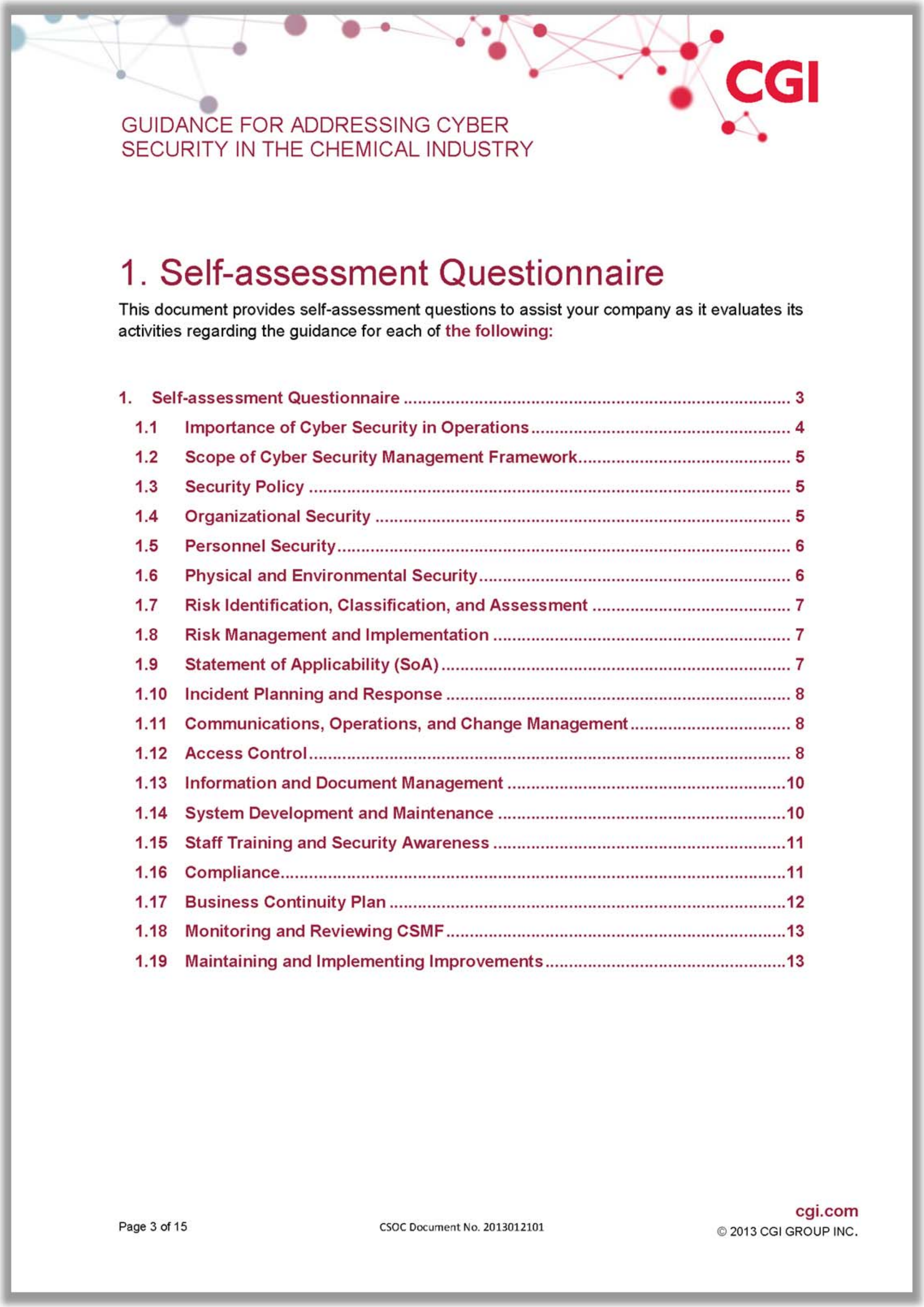
- It can provide the security functions that allow different zones to communicate securely.
- Any transfer of electronic data between zones must have a conduit.

Specific ICS Firewalls with DPI

ICS Firewalls are different compared to Standard Firewalls:

- ICS Firewalls have the facilities for Deep Packet Inspection to monitor and stop uncontrolled data transfer.
- ICS Firewalls can support different kind of specific low level transfer protocols.

cgi.com



GUIDANCE FOR ADDRESSING CYBER
SECURITY IN THE CHEMICAL INDUSTRY

1. Self-assessment Questionnaire

This document provides self-assessment questions to assist your company as it evaluates its activities regarding the guidance for each of the following:

Page 3 of 15

CSOC Document No. 2013012101

cgi.com

© 2013 CGI GROUP INC.

TO WHAT EXTENT IS CYBERSECURITY RISK INCORPORATED INTO ORGANIZATIONS’ OVERARCHING ENTERPRISE RISK MANAGEMENT?

Across the industry, CGI finds that cybersecurity risk is being incorporated into the overall enterprise risk management strategy and considerations. However, there are differing levels of maturity relative to not only the incorporate of cybersecurity into the enterprise risk management framework but also differing levels of maturity in how the outcomes of risk assessments are being evaluated, processes developed, and protocols implemented across organizations as it relates to IT and ICS cybersecurity.

CGI’s guidance to our clients is that, in order to understand the overall risks of an organization, a risk assessment should be undertaken at the corporate level as well as at plant level. At the plant/facility level, organizations need to assess the safety and security of the control systems operations in scope and examine the threats, impacts and vulnerabilities that the systems face not only relative to the plant itself but also to the overall organization. The risk assessments determines the most critical areas to address and provides the input for a selection process to ensure that the available resources are deployed in the areas where they achieve the most risk reduction.

In short, a combined assessment of the corporate risks as well as plant/facility risks needs to be analyzed holistically. Plant security risks must be aligned with the plant safety rules (as governed by OSHA, other government mandates, and industry-specific best practices), as security measures can sometimes conflict with plant safety procedures. Determination of legal requirements must support any trade-off analysis.

Once the business and safety risks are well understood, then a suite of risk reduction (security improvement) measures can be selected to form an overall secure architecture for the control systems environment.

WHAT STANDARDS, GUIDELINES, BEST PRACTICES, AND TOOLS ARE ORGANIZATIONS USING TO UNDERSTAND, MEASURE, AND MANAGE RISK AT THE MANAGEMENT, OPERATIONAL, AND TECHNICAL LEVELS?

The industry is quite familiar with the ISA and IEC standards; most are looking to those standards for guidance in formulating their cybersecurity frameworks and measures. However, selecting process control security measures is by no means an exact science, and ‘one size’ definitely does not fit all. Owing to the relatively immature nature of the field of process control security and the wide variety of legacy systems in existence, it is not just a simple matter of complying with international standards. There are a number of industry standards currently available across the industries, but we are far from a position of standardization relative to security protection measures.

CGI’s clients across the critical infrastructure sectors look to leverage standards and solutions that are already availability. They aim for commonality of approach to minimize cost and complexity. They look for reusability of proven solutions to reduce risks and costs associated with attempts to make solutions fit when unproven approached or technologies fail to provide the desired results. Our clients look to achieve multiple benefits from reuse of proven approaches and technologies:

- **Consistency of outcome through known quality standards** – reusing existing solution should ensure that the same level of quality is reproduced in different parts of the process control system or on different sites.
- **Easy to manage solutions** – if problems or exposures are handled the same way, then responding to incidents will be easier to manage as the same solution can be rolled-out to all process control systems that have used the same approach.

- **Economies of scale** – using a specific product or supplier across the organization may result in greater purchasing power and some influence over security design improvements.
- **Skills and expertise** – reusing proven control systems security approaches enables organizations to limit the development and training required to support the security measure. Third-party support costs can also be reduced.

As part of our SECURE-ICS approach, CGI has developed a series of SECURE-ICS Reference Guides for our clients that enable them to align their specific methodologies and solutions with industry best practices. Reference guides are applied in a modular fashion depending up on the industry, location of client (i.e., European standards under ENISE), and technologies employed within the ICS environment. A sampling of Reference Guide titles is provided in the table.

CGI SECURE-ICS Reference Guides

• ISO+31000-2009	• Security and Safety Standardization_TC65
• ISO+31000-2009	• ANSI-ISA 99-00-01_2007
• ISA 99 Standards to Improve Control Systems	• IEC 62443
• SCADA – Securing the Move to IP-Based SCADA PLC Networks	• Siemens Operational Guidelines – Industrial Security EN
• ENISA Protecting Industrial Security Controls	• Honeywell Security Solutions
• ABB Security for Industrial Automation and Control Systems	• Red Tiger Security NERC CIP and Other Frameworks
• NERC Security Guideline for the Electricity Sector	• Mission Critical Security in a Post Stuxnet World September 2011
• Control Systems Cyber Security Defense in Depth Strategies	• NSTB Lessons Learned from Cyber Security Assessments
• Chemical Sector Cyber Security Program Guidance Document	• Secure ICS Self-Assessment Questionnaire – Chemical Industry
• Security for Operators Plants	• SCADA Generic Risk Management Framework
• NIST Guide to Supervisory and Data Acquisition – SCADA and Industrial Control Systems Security	• Secure Information Communication Technologies Forward Whitebook
• Control System Cyber Security Self-Assessment Tool (CS2SAT)	• CPNI Good Practices SCADA Implement Secure Architecture

Throughout the implementation of the risk reduction measures there are a number of areas to consider:

- **Change control** – all changes to control systems should be carried out under the appropriate change control systems, as these changes may impact both the control systems and IT systems. Further down the value chain, the changes might need to be managed under different change systems such as for the plant systems and for the IT systems. As changes are made, the change control systems should ensure that the system diagrams, inventory and risk assessments are updated. If the change processes do not ensure these updates are made, then checks should be undertaken to ensure all information is up to date.
- **Post implementation reviews** – once the risk reduction measures are implemented, an assurance exercise should be undertaken to ensure that the measures have been deployed in accordance with the design of the security architecture. This could take a variety of forms from an implementation checklist to full security reviews or audits.

Penetration testing should only been done under strict conditions (e.g. plant shutdowns) as it is not uncommon for this type of test to shutdown control systems and corrupt process plant controllers

- **Communications and awareness** – throughout the implementation process, it is important to provide appropriate communications so that appropriate stakeholders are aware of the latest status and developments in the implementation project.

The job of process control security is not finished when all the risk reduction measures have been implemented. This is only a milestone in the control system's security lifecycle. Ongoing tasks ensure that the control systems remain appropriately secured in the future. Organizations must:

- Keep policy, standards and processes up to date with current threats
- Provide ongoing assurance that the control systems are in compliance with the security policy and standards
- Ensure that all engineers, users and administrators are security aware and implement the processes and procedures in a secure manner
- Put in place an appropriate response capability to react to changes in security threats
- Manage third-party risk.

Regular audits help verify that the risk is being actively managed and that the established processes and procedures are being followed.

WHAT ARE THE CURRENT REGULATORY AND REGULATORY REPORTING REQUIREMENTS IN THE UNITED STATES (E.G. LOCAL, STATE, NATIONAL, AND OTHER) FOR ORGANIZATIONS RELATING TO CYBERSECURITY?

U.S. Federal regulatory and reporting requirements addressing cybersecurity can be complex, involving both securing of systems and fulfilling of appropriate federal and non-federal roles in protecting critical information systems. There is, as yet, no overarching framework legislation in place but many enacted statutes addressing various aspects of cybersecurity across various industries. Some notable provisions are found in the following federal Acts:

- The **Federal Information Security Management Act of 2002 (FISMA**) clarified and strengthened NIST and agency cybersecurity responsibilities, established a central federal incident center, and made OMB, rather than the Secretary of Commerce, responsible for promulgating federal cybersecurity standards.
- The **Homeland Security Act of 2002 (HSA)** gave the Department of Homeland Security (DHS) cybersecurity responsibilities in addition to those implied by its general responsibilities for homeland security and critical infrastructure.
- The **Federal Trade Commission Act (FTC Act) Section 5** prohibits unfair and deceptive trade practices. Section 5 is included because courts have found that unfair competition includes activity that would violate the Sherman or Clayton Acts.
- **Securities and Exchange Commission (SEC) 2011 guidelines** published by the Securities and Exchange Commission make clear that publicly traded companies must report significant instances of cyber theft or attack, or even when they are at material risk of such an event.
- The **Sarbanes-Oxley Act of 2002** requires annual reporting on internal financial controls of covered firms to the Securities and Exchange commission

Elsewhere, across regulated industry outside of specifically the critical infrastructure space, organizations from corporations to small businesses, from states to municipalities and tribes, are required to report certain data for regulatory compliance. Any number of these reporting requirements can include data related to critical infrastructure components, technologies, materials, or hazards that could impact critical infrastructure if not properly controlled (e.g., hazardous chemicals entering the food supply).

Under current law, all federal agencies have cybersecurity responsibilities relating to their own systems, and many have sector-specific responsibilities for critical infrastructure, such as the Department of Transportation for the transportation sector. Cross-agency responsibilities are complex.

Publicly traded companies are still subject to the SEC voluntary program for reporting cyber theft or attacks. While the SEC guidance does not require disclosure as a result of every data security breach or cyber-attack, the guidance does require registered companies to conduct regular reviews of risk factors, to assess the likelihood that a data security breach or cyber-attack could occur and the potential costs of such a breach or attack. This review should take into account:

- the nature of the company’s business
- whether it is a target for cyber-attacks and hacking
- the sophistication of the company’s data security defenses
- threatened attacks of which the company is aware

Within increased regulatory action comes increased reporting requirements for industry and affected governmental agencies—regulatory reporting compliance requirements that can drive up costs to deliver critical services. Wherever possible, NIST’s framework should minimize duplicative reporting efforts in order to minimize financial burden, as those financial resources can be better used by organizations to reduce cyber threats proactively.

Another challenge is the timely gathering, analysis, evaluation, and publication of important information gathered from reporting. CGI brings lessons learned from developing other critical federal information sharing and publication initiatives (such as the Recovery Board’s FederalReporting.gov and the Environmental Protection Agency’s Central Data Exchange programs) to support the government in addressing future information sharing and publication requirements borne from new legislation or requirements resulting from the Framework.

WHAT ORGANIZATIONAL CRITICAL ASSETS ARE INTERDEPENDENT UPON OTHER CRITICAL PHYSICAL AND INFORMATION INFRASTRUCTURES, INCLUDING TELECOMMUNICATIONS, ENERGY, FINANCIAL SERVICES, WATER, AND TRANSPORTATION SECTORS?

The interdependencies between and among critical physical and information infrastructure cannot be underemphasized.

We identify organizational critical assets as people, information, technology, and facilities supporting critical functions. As such, we consider first level interdependencies (those with a most obvious correlation) as well as sub-level interdependencies (those that may not have immediate impact but, rather, cascading affect).

An attack on a dam can negatively impact any number of other sectors, as telecommunications, power, water, financial, health, and government buildings may be negatively impacted. An attack on the financial industry – for example, a cyber attack against the New York Stock Exchange – would impact every critical infrastructure sector in the U.S., with truly global implications.

WHAT PERFORMANCE GOALS DO ORGANIZATIONS ADOPT TO ENSURE THEIR ABILITY TO PROVIDE ESSENTIAL SERVICES WHILE MANAGING CYBERSECURITY RISK?

Performance goals to ensure ability to provide essential services vary, of course, by sector. Defining those minimum services and capabilities that define the “essential services” in, for example, a continuity of operations perspective varies not only by sector but company size and maturity. For large companies, especially those that are publicly traded, the risks associated with inability to provide essential services are weighed not only from a revenue perspective but a market perspective in terms of shareholder confidence and stock market value. For smaller companies, inability to provide essential services could result in catastrophic loss, including business closure. On the other hand, depending upon the sector, market, products/services, and customer base, inability to provide services for a set timeframe could have little to no impact on its financial viability.

Increasingly, the delta between essential services capability in COOP situations is being further impacted by the cyberinsurance market. As recently reported in “USA Today,” small companies can obtain cyberinsurance to cover liability for as little as $3,000[2] – significantly less investment than implementing cybersecurity technologies for continuous monitoring, for example. These cybersecurity insurance policies can cover claim response, mitigation of business interruption, breach monitoring services, forensic/investigative services post-breach, public relations support, as well as payment of ultimate liability (including payment of regulatory fines as a result of breach).

Across the industries we support, CGI sees a broad spectrum of definitions for essential service availability and performance. Those organizations that contract with CGI for consultation, assessment, or operational cybersecurity services tend to have a more mature risk management structure and strategy, but all are driven by financial implications. They weigh cost of cybersecurity investments in services and solutions (including creation of more mature standards and policies on the enterprise level) against potential loss (from a services, investment, and regulatory perspective).

IF YOUR ORGANIZATION IS REQUIRED TO REPORT TO MORE THAN ONE REGULATORY BODY, WHAT INFORMATION DOES YOUR ORGANIZATION REPORT AND WHAT HAS BEEN YOUR ORGANIZATION’S REPORTING EXPERIENCE?

CGI Federal is a member of the Defense Industrial Base (DIB). As a member, we are responsible for collaborating and sharing threat indicators with the government. CGI Federal shares and collaborates with the DIB with no issues or challenges.

WHAT ROLE(S) DO OR SHOULD NATIONAL/INTERNATIONAL STANDARDS AND ORGANIZATIONS THAT DEVELOP NATIONAL/ INTERNATIONAL STANDARDS PLAY IN CRITICAL INFRASTRUCTURE CYBERSECURITY CONFORMITY ASSESSMENT?

National and international standards must provide practical guidance and support in defining, implementing, assessing and monitoring secure IT and ICS environments based on best practices. A Cyber Security Management Framework supported by IT and ICS cybersecurity policies and requirements will be helpful in that case.

Industry specific implementations of these policies and requirements for levels 0 and 1 of the ISA 99 standard are important to address industry-specific needs.

It should be noted that new versions of several of the ISO 27000 standards are due for up-issue in late 2013. CGI has been part of the reviewing group for the new standards and have submitted our recommendations.

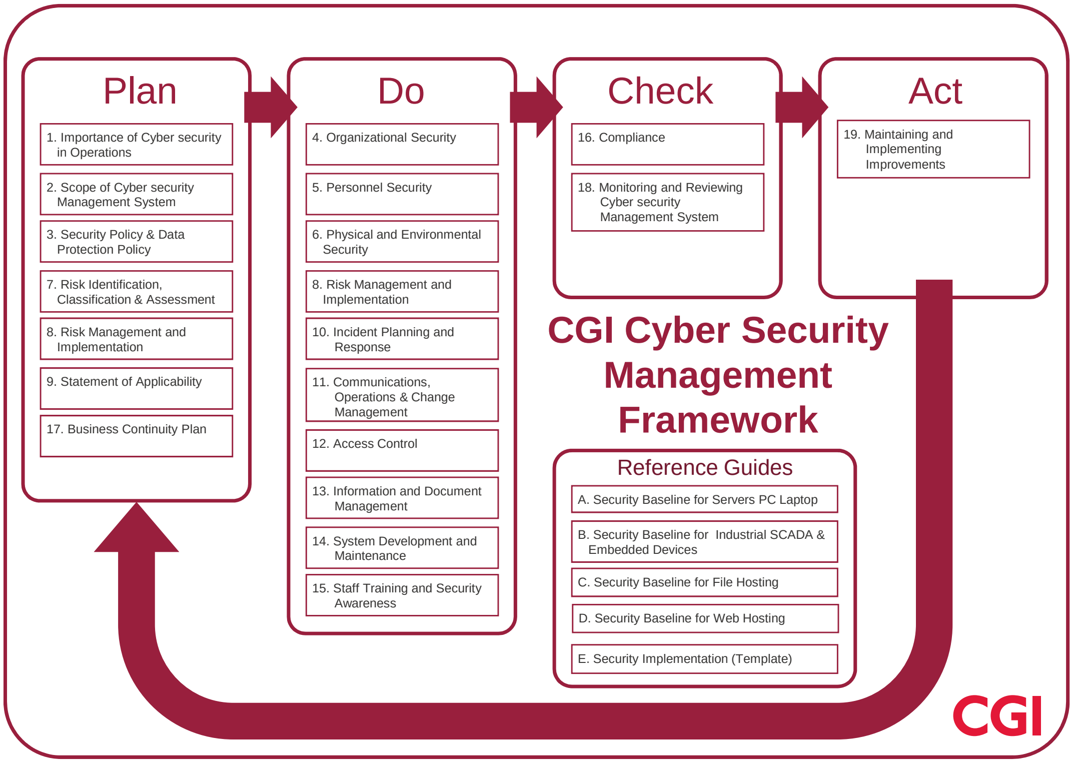
[2] http://www.usatoday.com/story/tech/2013/03/01/cyberinsurance-cyberattacks-small-businesses/1954399/

WHAT ADDITIONAL APPROACHES ALREADY EXIST? WHICH OF THESE APPROACHES APPLY ACROSS SECTORS? WHICH ORGANIZATIONS USE THESE APPROACHES?

A number of international standards and best practices exist and are widely used across industries today. Core standards include ISA-99, IEC 65C/WG10 for security for industrial process measurement and control – network and system security, the NIST 800 series, and Centre for the Protection of National Infrastructure (CPNI) best practices. Associated standards specific to the SCADA environment include AGA-12 for cryptographic protection of SCADA communications, API-1164 for pipeline SCADA security, Chemical Industry Data Exchange (CIDX) standards, and IEEE P1686 for substation IED cybersecurity and IEEE P1689for serial SCADA links and IED remote access.

As previously described, CGI has developed a Cyber Security Management Framework is based on the Guidance for Addressing Cyber Security in the Chemical Industry of the American Chemistry Council's, the Chemical Information Technology Council (ChemITC)™ and the Chemical Sector Cyber Security Program. The Cyber Security Management Framework presented uses elements of the BS 7799-2:2002. It also incorporates elements of ISO/IEC 17799, Information Technology Code of Practice for information security management as well as the concepts of the ISA 99 and the IEC 62443 standards. This CSMF is designed to be tuned to the specific needs of industry sectors and has been leveraged by CGI clients across sectors to include chemical, energy (utilities), and manufacturing.

Incorporating risk management practices including the Plan-Do-Check-Act approach, the CSMF incorporates both IT and ICS security requirements for critical infrastructure.


Plan
1. Importance of Cyber security in Operations
2. Scope of Cyber security Management System
3. Security Policy & Data Protection Policy
7. Risk Identification, Classification & Assessment
8. Risk Management and Implementation
9. Statement of Applicability
17. Business Continuity Plan
Do
4. Organizational Security
5. Personnel Security
6. Physical and Environmental Security
8. Risk Management and Implementation
10. Incident Planning and Response
11. Communications, Operations & Change Management
12. Access Control
13. Information and Document Management
14. System Development and Maintenance
15. Staff Training and Security Awareness
Check
16. Compliance
18. Monitoring and Reviewing Cyber security Management System
Act
19. Maintaining and Implementing Improvements
CGI Cyber Security Management Framework
Reference Guides
A. Security Baseline for Servers PC Laptop
B. Security Baseline for Industrial SCADA & Embedded Devices
C. Security Baseline for File Hosting
D. Security Baseline for Web Hosting
E. Security Implementation (Template)
CGI

The CSMF provides for comprehensive management of cybersecurity. It is an overall cybersecurity management framework that allows organizations adopting the CSMF to tailor it to its own specific needs.

The CSMF shows the main process steps in implementing Cyber Security in Industrial Environments while the Reference Guides support more specific the content (requirement) part of the most important items to address in plant Computer Infrastructure Control Networks (CICN) and the different devices. CICN Security Policies guide as well as a data protection policy guide supports the plant/facility managers and operators in a more general way, while reference guides support more specific topics and roles in the implementation of the security requirements.

Designed as a tailorable framework, modular and nature, built upon ICS cybersecurity concepts and architectures underpinned by industry best practices and standards, CGI sees no limitations to the use of CSMF across multiple sectors.

WHAT, IF ANY, MODIFICATIONS COULD MAKE THESE APPROACHES MORE USEFUL?

Cybersecurity in information technology and industrial control systems environments best practices must be shared along industries; modifications based on best practices are always welcome to enhance the approach.

HOW DO THESE APPROACHES TAKE INTO ACCOUNT SECTOR-SPECIFIC NEEDS?

Most of the time, sector specific needs will be addressed at the ISA 99 level 0, 1 and 2. Industry-specific publications about cybersecurity as well as vendor publications about specific industry implementations are incorporated in CGI's Reference Guides.

WHAT CAN THE ROLE OF SECTOR-SPECIFIC AGENCIES AND RELATED SECTOR COORDINATING COUNCILS BE IN DEVELOPING AND PROMOTING THE USE OF THESE APPROACHES?

Sector-specific agencies can play a key role in coordinating the development and promotion of best practices within their sectors and across sectors, driving improvements in approaches to prevention, protection, mitigation, response, and recovery. Sector-specific agencies and related sector coordinating councils can coordinate the industry-specific efforts, publish industry-specific best practices and trends, and provide recommendations about cybersecurity aligned with an industry-generic CSMF.

As sector-specific agencies and related coordinating councils look to support development and propagation of standards and best practices, they must weigh the value of voluntary programs as compared with regulatory programs in achieving desired objectives. Because increased regulatory action and necessary compliance programs have significant financial impacts for industry, any regulatory action should be restricted to those risks most critical to the nation's safety, prosperity, and well-being. The ISO 31000 risk management standard can support analysis of risk criticality, analyzed holistically not only in-sector but cross-sector. In this way, sector-specific agencies must appropriately represent their sectors in cross-coordination efforts specific to risk analysis and evaluation.

Regulatory and voluntary programs are only two of the ways in which sector-specific agencies can drive adoption of stronger cybersecurity standards. For example, provisions of the National Defense Authorization Act (NDAA) for 2013 require defense contractors to report data breaches (Section 941), with related DFAR requirements added to DoD solicitations for minimum capability of defense contractors to defend their IT networks. In this case, the government has identified means to adopt best practices through other incentives – the ability to be awarded government contracts – outside of the traditional regulatory or voluntary programs.

Other incentives that sector-specific agencies may work to bring to bear include tax considerations, decreased liability, and relief from existing regulations, such as those related to sharing SEC and/or FTC-restricted business information related to cybersecurity risks.

WHAT OTHER OUTREACH EFFORTS WOULD BE HELPFUL?

Creating communities of experienced cybersecurity experts – especially in the areas related to ICS – will enable industry across sectors to share best practices. Such efforts can be coordinated in close cooperation with and build upon the training efforts currently provided by the USA ICS Cyber Emergency Response Team (CERT) of the Department of Homeland Security. Furthermore, sector-specific agency outreach can include additional sector-specific knowledge transfer, coalition-building, and training to help drive adoption of best practices. As the same time, sector-specific agencies can look to existing or new capabilities to support threat identification, cybersecurity situational awareness within and across sectors, analysis of risk trends, evaluation of risk impacts, and other considerations through informal shared interest groups to formalized data gathering, analysis, and publication of threat trends via government-run data fusion centers.

Specific Industry Practices

ARE THESE PRACTICES WIDELY USED THROUGHOUT CRITICAL INFRASTRUCTURE AND INDUSTRY? HOW DO THESE PRACTICES RELATE TO EXISTING INTERNATIONAL STANDARDS AND PRACTICES? WHICH OF THESE PRACTICES DO COMMENTERS SEE AS BEING THE MOST CRITICAL FOR THE SECURE OPERATION OF CRITICAL INFRASTRUCTURE?

CGI’s SECURE-ICS approach is based on international best practices. CGI’s SECURE-ICS Reference Guide serves to document the international best practices in various critical infrastructure sectors, with emphasis on the utility, chemical, manufacturing, and water sectors. As guided by is documenting as much as possible the int. best practices for the electric (utility) sector, the chemical sector, the water sector, etc.

As guided by ISO 31000, we emphasize the importance of risk assessment in development of the security architecture for critical infrastructures. Part of these industry best practices is the importance of identifying/defining the secure zones and conduits within the security architecture. Specifically, an ICS security architecture needs to reflect the current state based on the information out of the asset management tools and an onsite plant/facility check of the current reality to assure the security architecture reflects the current environment.

The security architecture must be mindful of the following standards and principles:

- Defense in Depth (ISA 99 & IEC 62443)
- Separation of Concerns (ISA 99 & IEC 62443)
- People, processes & technology as a whole (ISA 99 & IEC 62443)
- Zones & Conduits (ISA 99 & IEC 62443)
- Safety and security cannot be separated
- Critical infrastructure environments typically operate on a 24x7x365 basis
- Critical infrastructure components often cannot be updated and tested during operations

Both physical security and cybersecurity are put in place with safety in mind. Cybersecurity protects control systems to keep the critical infrastructure processes working safely and efficiently. It ensures the data are not compromised. It keeps computer viruses, worms, Trojans, etc. from infecting the computers on the network and from affecting the control systems. It lets the right people access the controls and information, and it keeps the wrong people out of the controls, denying them access to sensitive, proprietary information and out of the network.

Based on best practices, the following topics are important to address in the context of securing critical infrastructure environments:

- **Increased Connectivity** – Today's ICS are being increasingly connected to company business systems that rely on common operating platforms and are accessible through the Internet. Even though these changes improve operability, they also create vulnerabilities because improvements in the security features of control systems are not concurrent.
- **Interdependencies** – Due to the high degree of interdependency among infrastructure sectors, failures within one sector can spread into others. A successful cyber attack might be able to take advantage of these interdependencies to produce cascading impacts and amplify the overall economic damage.
- **Complexity** – The demand for real-time control has increased system complexity in several ways: 1) access to ICS is being granted to more users business; 2) ICS are interconnected, and, 3) the degree of interdependency among infrastructures has increased. Dramatic differences in the training and concerns of those in charge of IT systems and those responsible for control system operations have led to challenges in coordinating network security between these two key groups.
- **Legacy Systems** – Although older legacy ICS may operate in more independent modes, they tend to have inadequate password policies and security administration. Further, they lack data protection mechanisms. Their protocols are prone to snooping, interruption, and interception. These insecure legacy systems have long service lives and will remain vulnerable for years to come unless these problems are mitigated.
- **System Accessibility** – Even limited connection to the Internet exposes ICS to all of the inherent vulnerabilities of interconnected computer networks, including viruses, worms, hackers, and terrorists. Control channels that use wireless or leased lines that pass through commercial telecommunications facilities may also provide minimal protection against forgery of data or control messages. These issues are of particular concern in industries that rely on interconnected enterprise and control networks with remote access from within or outside the company.
- **Offshore Reliance** – There are no feasible alternatives to the use of commercial off-the-shelf products in these ICS. Many software, hardware, and ICS manufacturers are under foreign ownership or develop systems in countries whose interests do not always align with those of the United States. Also of concern is the practice of contracting the support, service, and maintenance of ICS to third parties located in foreign countries.
- **Information Availability** – Manuals and training videos on ICS are publicly available, and many hacker tools can now be downloaded from the Internet and applied with limited system knowledge. Attackers do not have to be experts in control operations to create an impact.

WHICH OF THESE PRACTICES POSE THE MOST SIGNIFICANT IMPLEMENTATION CHALLENGE?

The biggest challenges tend to around management of the supply chain, particularly as out-sourcing and off-shoring become more common. This area is significantly enhanced in the new version of ISO/IEC 27002:2013.

DO ORGANIZATIONS HAVE A METHODOLOGY IN PLACE FOR THE PROPER ALLOCATION OF BUSINESS RESOURCES TO INVEST IN, CREATE, AND MAINTAIN IT STANDARDS?

As a large business with a significant global and government contract presence, CGI invests in the creation, establishment, and continuous refinement of our IT and security frameworks. We stay abreast of the latest IT standards, participating in discussions for standard creation and communities of interest for standard implementation. New standards play a significant role in driving our business investments and offerings to meet the regulatory requirements of our clients. For example, CGI invested significant capital and resources for creation of our CGI Federal Cloud environment to support our government clients. Build from the ground up to meet the specific security requirements for government hosting under NIST and government cloud hosting under both NIST and FedRAMP^{SM}, CGI's Federal Cloud achieved provisional authority to operate (P-ATO) by the FedRAMP Joint Authorization Board in January of 2013. We continue to work with FedRAMP's governing body and our clients to uphold the continuous monitoring requirements under FedRAMP and NIST 800-137.

DO ORGANIZATIONS HAVE A FORMAL ESCALATION PROCESS TO ADDRESS CYBERSECURITY RISKS THAT SUDDENLY INCREASE IN SEVERITY?

CGI advises its customers to implement formal escalation processes to address cybersecurity risks. These processes are part of plant managers and operators handbooks related to safety and security.

WHAT ARE THE INTERNATIONAL IMPLICATIONS OF THIS FRAMEWORK ON YOUR GLOBAL BUSINESS OR IN POLICYMAKING IN OTHER COUNTRIES?

When the framework is on a logical level with less restricted recommendations to U.S.-specific laws and regulations, then the framework could be easily used in another context/sector or geography. In recognition of the global marketplace and the number of international corporations with a role managing the U.S. critical infrastructure, tuning of the framework to country-specific laws and regulations must be easily done.

WHAT RISKS TO PRIVACY AND CIVIL LIBERTIES DO COMMENTERS PERCEIVE IN THE APPLICATION OF THESE PRACTICES? HOW SHOULD ANY RISKS TO PRIVACY AND CIVIL LIBERTIES BE MANAGED?

Current NIST guidance such as 800-122 and 800-144 (specific to cloud computing) provide relevant inputs to the critical infrastructure cybersecurity discussion. Further standards within the areas of public health have implication outside of the healthcare sector alone when considering the public health implications of attacks on water, agriculture, and other critical infrastructure sectors.

CGI POINTS OF CONTACT

The following CGI Subject Matter Experts contributed to this submission and welcome the opportunity to collaboration with NIST in discussions surrounding the Framework.

Please direct any questions regarding CGI's submission to:

David Sarmanian
CGI Federal Director Cyber Strategic Planning

Mr. Sarmanian leads CGI's U.S. Federal cybersecurity strategy practice, with 17 years of experience in Cyber Operations, Information Assurance and Information Systems Security. His areas of expertise include information security management, national security solutions, risk and compliance management, and disrupting/defending against advanced persistent threats.

david.sarmanian@cgifederal.com T: 703 365 8801

The following Subject Matter Experts welcome the opportunity further discuss international standards or sector-specific implications for the private sector:

Jaap Schekkerman
CGI Distinguished Management Consultant / Thought Leader
BTS, EA & Secure ICS

Jaap Schekkerman is a member of CGI's management consulting team and Thought Leader in Secure ICS environments, Enterprise Architecture Management, Services Orientation, and Cloud and Secure ICS environments. Mr. Schekkerman also serves as President and Thought Leader of the Institute For Enterprise Architecture Developments (IFEAD). He is a university lecturer and publisher of methods, articles and books on topics related to cybersecurity and enterprise architecture. He has coached and managed complex programs across the globe in the fields of defense, government, utilities, technology, healthcare, and oil and gas.

jaap.schekkerman@cgi.com T: 31 0 88 564 0000

Bruno Garrancho
CGI Cybersecurity Practice Leader, Portugal

Mr. Garrancho provides cybersecurity expertise to CGI's clients in Portugal and Spain with a focus on information security management, forensic techniques, risk management, and security testing. He holds a Master of Science in Information Technology – Information Security from Carnegie Mellon and a Master of Science in Information Security from the University of Lisbon.

bruno.garrancho@cgi.com T: 35 1 93 505 4083

cgi.com

Founded in 1976, CGI is a global IT and business process services provider delivering high-quality business consulting, systems integration and outsourcing services.