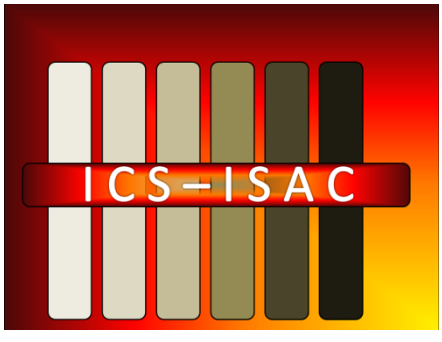
Response to NIST RFI:

"Developing a Framework to Improve Critical Infrastructure Cybersecurity"



Industrial Control System Information Sharing and Analysis Center

(ICS-ISAC)

April 1, 2013

Primary Contact:
Chris Blask
Chair
chris@ics-isac.org

Contents

Introduction

It is our position that maximum reduction of cyber risk to national critical infrastructure can only be achieved through improved operator control of industrial facilities and maximized knowledge sharing among involved parties. As facility operators can increase their technical and procedural ability to establish and maintain visibility into and control over the Industrial Control Systems (ICS) which manage their infrastructure they develop the ability to have knowledge of these systems. Where this knowledge can be shared appropriately without compromising personal and organizational privacy the United States can develop the situational awareness necessary to measure and manage national risk. Such a knowledge sharing system will support self-healing capabilities which will allow the national infrastructure to respond automatically to attack in an auto-immune fashion.

While vulnerability reduction, industry standards, workforce development and other methods play important parts in improving overall security none of these will lead to survivability of the national infrastructure against sophisticated active threats. The United States federal government, through this NIST Framework and other appropriate means, should support the development and adoption of human and technical capabilities which improve the ability for operators to have and maintain adequate control of their facilities and to engage in and benefit from appropriate knowledge sharing networks.

The Limits of Vulnerability Reduction

The millions of connected systems which today constitute American critical infrastructure face common challenges. These include pervasive vulnerabilities, the significant reduction of which will require extended periods of time and extensive capital investments. While actions aimed at reducing these vulnerabilities should be given due attention and resource, it must be understood that:

1. Given realistic resources, vulnerability reduction alone cannot reduce aggregate risk to an acceptable level at any point in the foreseeable future
    - Based on the vulnerability research to date which is available in the public domain it is reasonable to assume that virtually every deployed Industrial Control System device or piece of software contains exploitable vulnerabilities
    - The trained workforce of researchers necessary to identify a majority of vulnerabilities in all deployed ICS cyber devices in a reasonable and prudent period of time for these purposes does not exist
    - The necessity to “touch” every individual control system device found throughout every critical infrastructure facility in the nation in order to apply remediation to known vulnerabilities would mandate a workforce which is not available nor will be available under the most optimistic conditions for many years
    - It is unrealistic to assume that a single remediation of each ICS cyber device would be adequate to ensure all knowable vulnerabilities have been addressed in all deployed devices

2. Even with unlimited time and resources vulnerability reduction alone cannot reduce the aggregate risk to an acceptable level
    - even if the aforementioned resource restraints could be overcome and all reasonably knowable cyber vulnerabilities to all deployed devices and software could be discovered and remediations applied, all deployed systems would remain susceptible to all "Zero Day" vulnerabilities discovered by threat actors
    - the publically-known attacks against critical infrastructure to date have employed such Zero Day vulnerabilities, and therefore would have been successful even if all known vulnerabilities to the target systems had been remediated

Improving Operator Control of Industrial Facilities

It is within the reasonable reach of facilities to improve their control over their cyber systems given existing fiscal limits and within appropriate periods of time. Such control can be implemented without causing unacceptable negative impact to the current safety, reliability and availability of such systems. This can be accomplished with technology currently available in both commercial as well as Open Source forms. The operational characteristics of the organizations which own and manage the majority of these systems lends themselves to the adoption of such control capabilities.

Organizational Characteristics Supporting Cyber Controls

A common characteristic of organizations in many critical infrastructure sectors is a core focus on situational awareness. Physical, electrophysical and cyber Industrial Control Systems have been developed for the specific purpose of providing facility operators maximum situational awareness of the state of the physical process being managed. These organizational characteristics support the development of operational processes to establish and maintain situational awareness of the cyber systems at the core of this issue much more so than among Information Technology (IT) organizations.

In the effort to secure infrastructure a common commentary is to the effect that Industrial Control System networks are not able to utilize many of the methods of security prevalent in Information Technology (IT) applications. Methods as basic as the application of software patches become extremely problematic in ICS environments where the consequence of such a patch causing a fault may be higher and more likely than the problem fixed by the patch, or where no "off hours" window of opportunity to apply such patches presents itself. In the singular area of Situational Awareness, however, ICS environments are often more amenable to the use of such processes and technologies than are IT.

IT networks are characteristically complex and dynamic. Devices, users, applications and traffic patterns may change from moment to moment without the direct and explicit knowledge of the network operators. Establishing situational awareness on IT networks is a significant area of focus in enterprises today, but it is continuously challenged to address the "high false positive" aspect of discriminating between "bad changes" which indicate risks and threats and "good changes" which are simply artifacts of permitted enterprise activity.

In industrial settings on ICS networks, changes in users, devices and applications are generally rare and occur under controlled circumstances. Traffic patterns on these networks in the overwhelming majority of instances are deterministic and relatively low-volume, following predictable cycles explicitly known to system designers and operators. The application of situational awareness technologies currently available therefore require less customization and operational attention in ICS environments than in IT.

From a workforce perspective, the operational processes used by industrial system operators are oriented specifically towards maintaining situational awareness of the subject physical process. Whether manufacturing, energy, transportation, water or other sector-specific area the operational process in place has been designed with the singular attention to continuous awareness of the state of the physical process. This sociological focus lends itself to the adoption of the processes required to establish and maintain situational awareness of cyber systems very directly, whereas in IT environments such processes often run counter to enterprise operations.

Technical Methods for Maintaining Situational Awareness

Where facility operators do not have the ability to know definitively what their cyber control systems are composed of and what these systems are doing they can possess no effective knowledge as to the security state of these systems. Where facilities lack the capability to have and maintain this knowledge they will remain unable to effectively apply knowledge shared with them by external parties, and also unable to have knowledge which can be shared with appropriate external parties. Where this remains the common state among facility operators, there can be no national awareness of the state of the cybersecurity of our aggregate infrastructure nor ability to take effective action in its defense.

There exist today multiple technical methods which can be employed to create and maintain appropriate situational awareness of cyber control systems. These methods exist in Open Source as well as commercial forms, providing facility owners and operators sufficient selection to identify and acquire appropriate tools to serve this purpose at their sites. The adoption and deployment of these technical tools and methods can provide the organizations achievable means around which to build operational processes.

There are two major components of situational awareness of cyber control systems:

Inventory:
: A current and accurate inventory of all software and hardware components of the Industrial Control System.

Activity:
: An accurate awareness of past and present cyber activity within and between the Industrial Control System components.

For a facility operator to maintain situational awareness it is necessary to have the capability to:

- establish an initial baseline of Inventory and Activity
- validate this baseline against the intended composition and behavior of the subject control system
- maintain a capability to determine when divergence from this baseline occurs

Technical methods of establishing and maintaining situational awareness must in all cases take into account the priorities of the subject facility. Availability, safety and reliability considerations dictate that the tools

used to establish and maintain situational awareness are implemented in such ways that they have minimal-to-no actual or potential impact on the currently deployed infrastructure. This can include the deployment of such monitoring technologies on network segments separate from the operational control system and the "mirroring" of the activity of the deployed cyber control system to these separate segments.

It is recommended that for the purpose of the NIST Framework specific technologies not be mandated or promoted, rather that methods be investigated to promote or as necessary mandate the adoption of technical and process mechanisms for maintaining appropriate situational awareness and detecting unauthorized inventory and/or activity alteration.

Knowledge Sharing

To achieve the goal of a survivable infrastructure it is mandatory that we develop the capability to create and maintain awareness of the ongoing aggregate state of national infrastructure. At present there is no adequate capability to determine whether the infrastructure of the United States is or is not under active attack by threat actors - either in a broad sense or with any specificity - at a given point in time or over a given span of time. While securing the individual facilities which together comprise national infrastructure is necessary, the national ability to determine the overall state of security across infrastructure remains a separate and distinct need. This need can be addressed through the development of appropriate Knowledge Sharing methods.

Similar with individual facilities, where the United States as a nation has no means of determining the Inventory nor Activity of its infrastructure there is no capacity for having Knowledge of the risks or threats to national security. Unlike individual facilities, it is not as fundamental a requirement to establish as precise and detailed a situational awareness of national infrastructure to achieve effective national situational awareness. Appropriately defining the mechanisms used and content shared across the National Knowledge Sharing Network are the crucial factors in building an effective national defense.

Knowledge Sharing Mechanisms

Knowledge Sharing Mechanisms fall into two basic categories:

- Human-to-human knowledge sharing
- Machine-to-machine (automated) knowledge sharing

To achieve a secure and reliable national infrastructure our ability to share knowledge must increase exponentially in both areas. Strategic and tactical planning by human operators and policy makers must always be informed by then-current realities and best practices. Our trained workforce must expand exponentially from current levels to provide the capacity to apply and maintain any viable solutions, while continuously improving itself in a highly dynamic environment. Our infrastructure itself must become significantly more autonomous and connected, increasing its ability to detect and respond to threats at a speed and with a reliability that will rapidly become beyond human operators' capability.

Fortunately, the groundwork for advancing human and automated knowledge sharing has already been laid. The forward-looking efforts necessary are largely the increased adoption and utilization of processes, technologies and techniques which have been developed and demonstrated.

Human Knowledge Sharing

Human-to-human knowledge sharing methods include communications among and between peer groups. There has been significant progress to date developing human-to-human information sharing mechanisms. From in-person sessions to web-based and other virtual information human sharing mechanisms to the creation of the ISAC structure to facilitate public-private collaboration in concert with US-CERT, a substantial foundation has been laid. In addition, a peer-to-peer network of those directly involved in Industrial Control System operation and function has developed organically.

The information dissemination mechanisms developed to date on average remain challenged to address issues of timeliness and scale, however. We must continue to broaden the demographic reach and expand mechanisms used. Direct sharing of critical information between members of confined circles of trust needs to continue, but sufficient knowledge to perform component tasks must be disseminated to students preparing to contribute to the workforce as well as millions of workers currently involved with operating infrastructure.

The existing human-to-human information sharing work being done by public and private sector parties should be analyzed for effectiveness and where successful increased in scale and reach. Untapped communities of interest across all infrastructure sectors should continue to be brought into these mechanisms and conversations through all means including industry trade organizations, publications and conferences. Educational institutions should be further involved in propagating skills and knowledge to the diverse workforce needed to securely design, build and operate the increasingly automated and interconnected infrastructure of today and tomorrow.

This is in no way to diminish the incredible importance of human-to-human information sharing as it will remain a key component moving forward. Continuing to expand and build upon these efforts is crucial to long term success and viability of the critical infrastructure system.

Automated Knowledge Sharing and the Self-Healing Infrastructure

While human-to-human knowledge sharing is a critical component to inform strategy and tactics among decision makers and perform workforce development, it cannot ultimately be performed at speeds adequate to facilitate national defenses against large scale sophisticated attacks alone. During periods of military conflict or other foreseeable conditions of lesser but still substantial conflict with well-resourced threat actors our interdependent national infrastructure will require “self-healing” capabilities only possible through automated knowledge sharing. It is within the reach of the United States to implement such automated knowledge sharing systems based on existing technical and organizational developments. NIST and the US federal public sector should work to enable and accelerate where possible advancements in and adoption of such automated knowledge sharing systems.

Machine-to-machine knowledge sharing provides the opportunity to build a responsive national infrastructure capable of maintaining stability during periods of active attack. Work in various areas in

recent years has provided a rich technical and operational foundation from which such an automated national network can be implemented. Development of standards for this purpose has reached fairly robust maturity and examples of operable automated defensive networks have been deployed for a number of years. By supporting the further development and deployment of reference architectures utilizing these methods the public and private sectors together have the opportunity to demonstrate replicable structures which can be broadly adopted.

An example of effective automated knowledge sharing deployed today is the Collective Intelligence Framework (CIF) created by the Research and Educational Network Information Sharing and Analysis Center (REN-ISAC). Where a CIF member detects for example an email address used in Phishing attacks or an IP address performing denial of service attacks, this information is shared with all other members whose systems may automatically block or watch for traffic so indicated. The Structure Threat Information eXpression (STIX) standard for representing threat indicators and the Trusted Automated eXchange of Indicator Information (TAXII) standard for securely exchanging threat information build on years of industry experience with automating knowledge sharing. All of these and other existing, developing, open and proprietary standards for threat representation and transportation provide technical options for machine-to-machine knowledge sharing which can be used to develop and exercise reference architectures capable of providing active defenses.

It is well within our reach - using current technologies - to create an infrastructure where an attempt to compromise industrial facilities results in immunity to such an attack being propagated automatically to all other vulnerable facilities. Enabling situational awareness at industrial and infrastructure facilities and connecting these facilities appropriately with public and private sector knowledge sharing and analysis centers can provide this national defensive capability.

Building Repeatable Reference Architectures

As there exists a significant mass of technology and expertise in the nation today which can be used to achieve the goals of securing critical infrastructure there is a value in enabling vendors, practitioners and other subject matter experts in efforts to validate, demonstrate and disseminate repeatable reference architectures. In the public and private sector exist groups capable of - and in some cases in the process of – building such reference architectures. NIST and other public sector entities at the state and federal level should take what actions reasonably achievable to support such exercises and to propagate demonstrated successes.

A great deal of progress on most, or perhaps even all, of the component challenges to infrastructure threat has been accomplished. Over the past two decades technical and procedural capabilities have consistently evolved in a positive direction and in recent years efforts have produced a plethora of applicable tools, structures and expertise. There exist individual organizations and consortia capable of performing both large as well as small-scale demonstration projects which can definitively prove or disprove methods for addressing aspects of the overall challenge. Existing groups of state, local and/or federal public sector authorities are currently engaged with pertinent private sector entities and capable of working together to perform demonstrations of local, regional and/or national defenses. NIST and the US federal public sector should as appropriate foster and enable such demonstrations of replicable reference models which can be adopted with a high degree of reliability.

Summary

NIST and the US federal public sector have a pivotal role to play in realizing the goal of a national infrastructure capable of remaining intact under coordinated and sophisticated cyber attack. Associated risks have a strong potential to continue to escalate from their current significant level to become clear and present dangers to the on-going stability of the nation, and to do so within the period of time necessary to enact adequate countermeasures and capabilities. The Framework to achieve this goal looking forward from the present must recognize existing progress made while executing on the opportunity to establish a system of national situational awareness and response.

Subject matter experts and private sector entities as well as local, state and regional public sector organizations are well prepared and poised to develop and deploy the human and automated knowledge sharing mechanisms necessary to achieve the national goal. Inasmuch as NIST and the US federal public sector is able to empower and harness these opportunities and abilities it is very much within our national grasp to implement the systems and educate the workforce required to make the American infrastructure an open yet robust platform for societal and economic growth. The US has a unique opportunity at this point in history to create the national reference model of modern infrastructure and lead global development in a field which will define the century.