ICS-CERT MONITOR

January – April 2014

NCCIC

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

## CONTENTS





**Contact Information**

For any questions related to this report or to contact ICS-CERT:
Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585

I Want To
- Report an ICS incident to ICS-CERT
- Report an ICS software vulnerability
- Get information about reporting

Downloading PGP/GPG Keys
http://ics-cert.us-cert.gov/sites/default/files/documents/ICS-CERT.asc

**Joining the Secure Portal**

ICS-CERT encourages U.S. asset owners and operators to join the Control Systems compartment of the US-CERT secure portal. Send your name, telephone contact number, email address, and company affiliation to ics-cert@hq.dhs.gov requesting consideration for portal access.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/

## INCIDENT RESPONSE ACTIVITY

# INTERNET ACCESSIBLE CONTROL SYSTEMS AT RISK

Is your control system accessible directly from the Internet? Do you use remote access features to log into your control system network? Are you unsure of the security measures that protect your remote access services? If your answer was yes to any or all these questions, you are at increased risk of cyber attacks including scanning, probes, brute force attempts and unauthorized access to your control environment.

Internet facing devices have become a serious concern over the past few years with remote access demands giving way to insecure or vulnerable configurations. Tools, such as SHODAN, Google and other search engines, enable researchers and adversaries to easily discover and identify a variety of ICS devices that were not intended to be Internet facing. Adding to the threat landscape is the continued scanning and cataloguing of devices known to be susceptible to emerging vulnerabilities such as the OpenSSL "Heartbleed." In addition, the search terms needed to identify ICS devices are widely available because of an increasing public body of knowledge with detailed ICS-specific terminology. The availability of this information, coupled with the aforementioned tools, lowers the level of knowledge required to successfully locate Internet facing control systems.

In many cases, these devices have not been configured with adequate authentication mechanisms, thereby further increasing the chances of both opportunistic and targeted attempts to directly access these components. As tools and adversary capabilities advance, we expect that exposed systems will be more effectively discovered, and targeted by adversaries. Clearly, it has become more important for asset owners and operators to audit their network configurations and properly install their ICS devices behind patched VPNs or firewalls.

Most recently, ICS-CERT received reports of three new cyber incidents that resulted from weak network configuration and/or lack of perimeter security. Two of those incidents involved intrusions by unauthorized parties, and the other was identified as vulnerable by a researcher. In the majority of these cases, the system owners are unaware of the nonsecure configurations or the associated risk.

### Public Utility Compromised

A public utility was recently compromised when a sophisticated threat actor gained unauthorized access to its control system network. After notification of the incident, ICS-CERT validated that the software used to administer the control system assets was accessible via Internet facing hosts. The systems were configured with a remote access capability, utilizing a simple password mechanism; however, the authentication method was susceptible to compromise via standard brute forcing techniques.

ICS-CERT provided analytical assistance, including host-based forensic analysis and a comprehensive review of available network logs. It was determined that the systems were likely exposed to numerous security threats and previous intrusion activity was also identified. ICS-CERT conducted an onsite cybersecurity assessment in response to

this incident to assist the asset owners with evaluating the overall security posture of their infrastructure. In addition, ICS-CERT made practical recommendations for re-architecting and securing the control network. This incident highlights the need to evaluate security controls employed at the perimeter and ensure that potential intrusion vectors (ex: remote access) are configured with appropriate security controls, monitoring, and detection capabilities.

**Control Systems Device Remotely Accessed by Threat Actor**

The second example involved an unprotected, Internet-connected, control system operating a mechanical device. Upon investigation, ICS-CERT determined that a sophisticated threat actor had accessed the control system server (connected via a cellular modem) through a supervisory control and data acquisition (SCADA) protocol. The device was directly Internet accessible and was not protected by a firewall or authentication access controls. At the time of compromise, the control system was mechanically disconnected from the device for scheduled maintenance. ICS-CERT provided analytic assistance and determined that the actor had access to the system over an extended period of time and had connected via both HTTP and the SCADA protocol. However, further analysis determined that no attempts were made by the threat actor to manipulate the system or inject unauthorized control actions. After the incident was resolved, ICS-CERT conducted an onsite cybersecurity assessment of its larger control environment to evaluate its security posture and make recommendations for further securing its remote access to its control network. This incident highlights the need for perimeter security and monitoring capabilities to prevent adversaries from discovering vulnerable ICSs and using them as targets of opportunity.

**Sochi Arena HVAC System Exposed to the Internet**

Billy Rios, a researcher at Qualys, provided information to ICS-CERT and various media outlets concerning an Internet facing HVAC and Energy Management System (EMS) associated with an arena at the Sochi Olympics in Russia. This system was reported to lack authentication requirements to access the control system. The researcher worked with the system integrator to reconfigure the system prior to the Olympics and opening ceremonies.

**What Should You Do?**

ICS-CERT strongly encourages taking immediate defensive action to secure ICSs by using defense-in-depth principles. Audit your networks for Internet facing devices, weak authentication methods, and component vulnerabilities. Understand the usage of tools, such as SHODAN and Google, and leverage those platforms to enhance awareness of the Internet accessible devices that might exist within your infrastructure.

ICS-CERT also recommends that users take defensive measures to minimize the risk of exploitation as follows:

- Minimize network exposure for all control system devices. In general, locate control system networks and devices behind firewalls and isolate them from the business network.
- When remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
- Remove, disable or rename any default system accounts wherever possible.
- Implement account lockout policies to reduce the risk from brute forcing attempts.
- Establish and implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.
- Apply patches in the ICS environment, when possible, to mitigate known vulnerabilities.

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for incident response support and correlation with other similar incidents. We urge critical infrastructure owners and operators to evaluate their systems and ensure that they are not directly accessible from the Internet.

ICS-CERT encourages organizations to reference the previously released alerts, which detail the risks associated with Internet-accessible ICS devices. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

a. ICS-ALERT-11-343-01 – Control System Internet Accessibility, http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-343-01A, web site last accessed February 27, 2014.

b. ICS-ALERT-10-301-01 – Control System Internet Accessibility, http://ics-cert.us-cert.gov/alerts/ICS-ALERT-10-301-01, web site last accessed February 27, 2014.

## RECAP OF VUNERABILITIES IN 2013

As previously reported in the 2013 Year in Review, ICS-CERT received 181 vulnerability reports from researchers and ICS vendors throughout the year. Of those, 177 were determined to be true vulnerabilities that involved coordination, testing, and analysis across 52 vendors. The majority of these or 87 percent were exploitable remotely while the other 13 percent required local access to exploit the vulnerabilities. A fundamental recommendation for mitigating remotely exploitable vulnerabilities is to minimize network exposure and configure ICSs behind firewalls so they aren't directly accessible and exploitable from the Internet. Equally important is patching and updating ICS devices as soon as practically possible, understanding that patches and upgrades must be properly tested by each asset owner/operator before being implemented in operational environments. The following chart depicts the different types of vulnerabilities reported and coordinated in 2013.

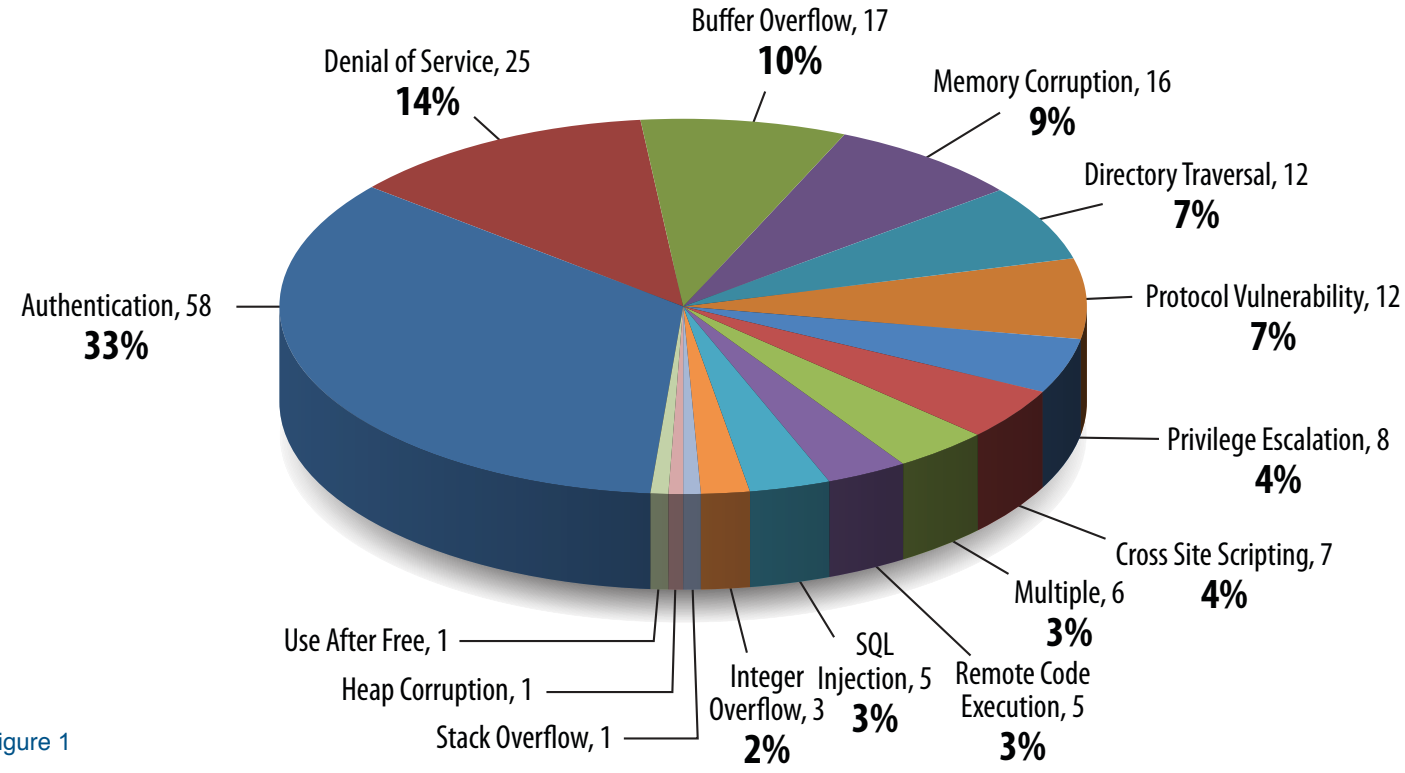


Figure 1

Authentication flaws were the most abundant vulnerability type coordinated in 2013, which includes vulnerabilities like factory hard-coded credentials, weak authentication keys, etc. These tend to be of highest concern because an attacker with minimal skill level could potentially gain administrator level access to devices that are accessible remotely over the Internet.

New for 2013 was the inclusion of medical device vulnerabilities as some researchers began to shift their efforts toward these devices. Instrumental in this shift was the relationship that ICS-CERT formed with the US Department of Health and Human Services, the US Food and Drug Administration (FDA) and multiple medical device manufacturers. One noteworthy example of these efforts was a report from researchers Billy Rios and Terry McCorkle who discovered a hard-coded password vulnerability affecting roughly 300 medical devices across approximately 40 vendors. The affected devices are manufactured by a broad range of vendors and fall into a broad range of categories, including but not limited to:

- Surgical and anesthesia devices,
- Ventilators,
- Drug infusion pumps,
- External defibrillators,
- Patient monitors and
- Laboratory and analysis equipment.

ICS-CERT continues to coordinate with multiple vendors, the FDA and the security researchers to identify specific mitigations across all devices. The FDA has published recommendations and best practices to help prevent unauthorized access or modification to medical devices.

Notable among many of the higher ranking vulnerabilities were the DNP3 vulnerabilities discovered by Adam Crain and Chris Sistrunk. These serious flaws affect certain implementations of the DNP3 protocol in various master-slave station products. These vulnerabilities, if exploited, could cause a denial-of-service (DoS) condition against the DNP3 master over either TCP/IP or serial communication paths, impeding the DNP3 master from communicating to field devices until remediated.

In response, ICS-CERT has been working with the affected vendors to create patches or updates to mitigate risk to attacks leveraging these vulnerabilities. To date, ICS-CERT has produced 18 advisories for various ICS devices. A comprehensive list of public DNP3 implementation vulnerabilities can be found in ICS-CERT Advisory ICSA-13-291-01B - DNP3 Implementation Vulnerability (Update B) (http://ics-cert.us-cert.gov/advisories/ICSA-13-291-01B) and in subsequent updates that will be released in the future.

## SCORING

Nearly 65 percent of the vulnerabilities that ICS-CERT coordinated in 2013 were scored and ranked as high priority vulnerabilities for asset owners and operators to mitigate in their systems. These vulnerabilities scored 7.0 or higher using the Common Vulnerability Scoring System (CVSS).

When calculating CVSS scores, ICS-CERT uses the National Institute of Standards and Technology (NIST) NVD CVSS Version 2 concise score calculator found at: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2. The base score is provided in the form of a CVSS vector string, which tells readers the variables that went into computing the score. An example of a vector string that equates to a base score of 10.0 is (AV:N/AC:L/Au:N/C:C/I:C/A:C). All advisories provide a link back to the NIST CVSS calculator that displays the base metrics (see Figure 2). Readers can combine information from the CVSS score, description of the vulnerability and exploit availability and apply this information to the best of their ability to their individual operating environment. ICS-CERT provides CVSS base scores as a tool for affected asset owners to aid them in prioritizing their mitigation strategies. Control system owners/operators are encouraged to customize the CVSS temporal and environmental metrics to calculate a total score that applies to their individual deployment characteristics. More information about CVSS scoring can be found at the FIRST CVSS web site.

The following chart shows the percentage of vulnerabilities in each of the severity ranges that ICS-CERT worked in 2013. Out of the 177 vulnerabilities, 93 have been documented and released in advisories and those 93 are represented below. The remaining 84 vulnerabilities are currently in open tickets that ICS-CERT is coordinating between researchers and vendors, and CVSS scores have not been determined for each of them yet.

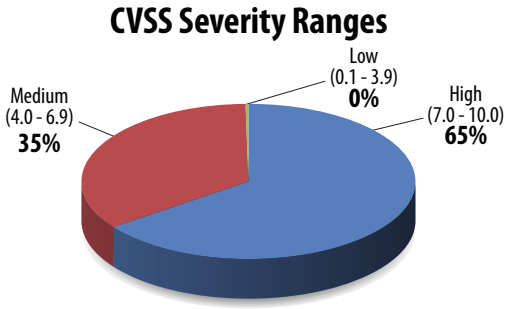


Figure 2

The list of researchers in Table 1 coordinated with ICS-CERT and contributed to making ICSs more secure in 2013. ICS-CERT appreciates their efforts and looks forward to continued engagement and coordination in 2014.

Table 1. Researchers that ICS-CERT coordinated with in 2013:

| | |
|---|---|
| Aaron Portnoy | Celil Unuver |
| Adam Crain | Cesar Cerrudo |
| Adam Todorski | Christopher Sistrunk |
| Andrea Micalizzi | Dallas Haselhorst |
| Anton Popov | Darius Freamon |
| Arthur Gervais | Derek Betker |
| Billy Rios | Dillon Beresford |
| Brian Meixell | Dylan Jenkins |
| Carlos Mario Penagos Hollman | Eireann Leverett |
| Carsten Eiram | Emmett Moore |
| Eric Forner | Positive Technologies Security |
| Hisashi Kojima | Reid Wightman |
| Joel Febrer | Rubén Santamarta |
| Joel Langill | Sanadi Antu |
| Jon Christmas | Said Arfi |
| Juan Vasquez | Siemens, ProductCERT |
| Lucas Apa | Sergey Gordeychick |
| Mashahiro Nakada | Stephen Dunlap |
| Mehdi Sabraoui | Terry McCorkle |
| Michael Toecker | Tom Gallagher |
| Mike Davis | Wei Gao |
| Nicholas Miles | ZDI |
| Neil Smith | |

## ICS-CERT ASSESSMENTS

The ICS-CERT Onsite Assessments & Assistance Program provided expert guidance and support to 20 Industrial Control Systems (ICS) owners and operators to complete Onsite Cybersecurity Evaluation Tool (CSET®) assessments, Design Architecture Reviews (DAR), and Network Engineering Verifications and Validations (NAVV).

- The Onsite CSET® assessment helps the asset owner identify primary vulnerabilities and improvements, as well as analyze the control system's core functions, infrastructure, policies, and procedures by using industry recognized standards.
- The DAR provides ICS owners and operators with a comprehensive evaluation and discovery process, focusing on defense strategies associated with the asset owner's specific control systems network.
- The NAVV provides a sophisticated analysis on the header-data captured and submitted voluntarily by ICS owners and operators to ICS-CERT.

Combined, these services have assisted ICS owners and operators from multiple states including Idaho, New York, California, Kansas, Arkansas, Indiana, and Connecticut and spanning multiple sectors including Energy, Water, Transportation Systems, and Government Facilities to improve their ICS security and resilience.

Table 2. ICS-CERT assessments first quarter of 2014.

| Quarter | Month | Year | Description | Type |
|---|---|---|---|---|
| 2 | January | 2014 | Energy Utility | Onsite CSET |
| 2 | January | 2014 | Energy Utility | Onsite CSET |
| 2 | January | 2014 | Water Utility | Onsite CSET |
| 2 | January | 2014 | Energy Utility | Onsite CSET |
| 2 | January | 2014 | Water Utility | Onsite CSET |
| 2 | January | 2014 | Water Utility | Onsite CSET |
| 2 | January | 2014 | Water Utility | Onsite CSET |
| 2 | January | 2014 | Water Utility | Design Arch Rev |
| 2 | February | 2014 | Water Utility | Onsite CSET |
| 2 | February | 2014 | Transportation Utility | Onsite CSET |
| 2 | February | 2014 | Transportation Utility | Onsite CSET |
| 2 | February | 2014 | Water Utility | Onsite CSET |
| 2 | February | 2014 | Water Utility | Design Arch Rev |
| 2 | February | 2014 | Water Utility | NAVV |
| 2 | March | 2014 | Water Utility | Onsite CSET |
| 2 | March | 2014 | Nuclear Facility | Onsite CSET |
| 2 | March | 2014 | Nuclear Facility | Design Arch Rev |
| 2 | March | 2014 | Nuclear Facility | NAVV |
| 2 | March | 2014 | Energy Utility | Design Arch Rev |
| 2 | March | 2014 | Water Utility | Onsite CSET |

## BASIC STEPS TO SECURE YOUR NETWORKS

Most of us lock our front doors when we leave the house. It is a simple way to increase the security of our home. In the same way, there are basic steps that should be taken to secure control systems. As part of the strategy to assist industry with securing critical control systems, ICS-CERT offers, and has conducted numerous onsite consultations, at no cost to asset owners. These engagements provide an opportunity for security experts to examine an organization's cybersecurity posture and report opportunities for the business to make improvements.

The assessment approach helps asset owners and operators to select the level of ICS-CERT support needed to meet their operational requirements. The assessment team has during the course of these assessments identified common vulnerabilities and weaknesses (see Table 2), from access controls to networking design, that critical infrastructure owners and operators must consider when assessing their infrastructure for potential threats and risks.

Table 3. Vulnerabilities and weaknesses identified by the assessment team.

| Category | Common Vulnerability |
|---|---|
| Permissions, Privileges, and Access Controls | Poor system access controls |
| Improper Authentication | Poor system identification/authentication controls |
| Credentials Management | Insufficiently protected credentials |
| | Weak passwords |
| Security Configuration and Maintenance | Weak testing environments |
| | Poor patch management-limited patch management abilities |
| | Weak backup and restore capabilities |
| Planning/Policy/Procedures | Poor security documentation and maintenance |
| | Lack of formal documentation |
| | Insufficient disaster recovery penetration |
| Network Design Weaknesses | Common ICS network design weaknesses |
| | No security perimeter defined |
| | Lack of network segmentation |
| | Lack of functional DMZs |
| | Firewalls nonexistent or improperly configured |
| Network Component Configuration (Implementation) Vulnerabilities | Network devices not properly configured<br>Port security not implemented on network equipment |

## SITUATIONAL AWARENESS - Continued

A commonly observed challenge and one of the easiest to address is a flat network topology. A risk associated with a flat network is the absence of logical segmentation, which serves to restrict communications originating from one portion of a network to another portion of the same network, for example that of a standard corporate/business network to the controls systems network. In a flat or nonsegmented network topology, communications will be uninhibited and able to traverse across all elements within the network. Figure 3 illustrates how segmenting and implementing a demilitarized zone (DMZ) adds security by limiting the communication paths on the network.

A DMZ is a semi-trusted zone that acts as a buffer between network segments. Business networks often place public facing systems like web servers in a DMZ between their trusted business network and the Internet. In control systems, a DMZ should exist between the business network and the control systems network. In addition, a DMZ should be established between the control system network and any other network segments.

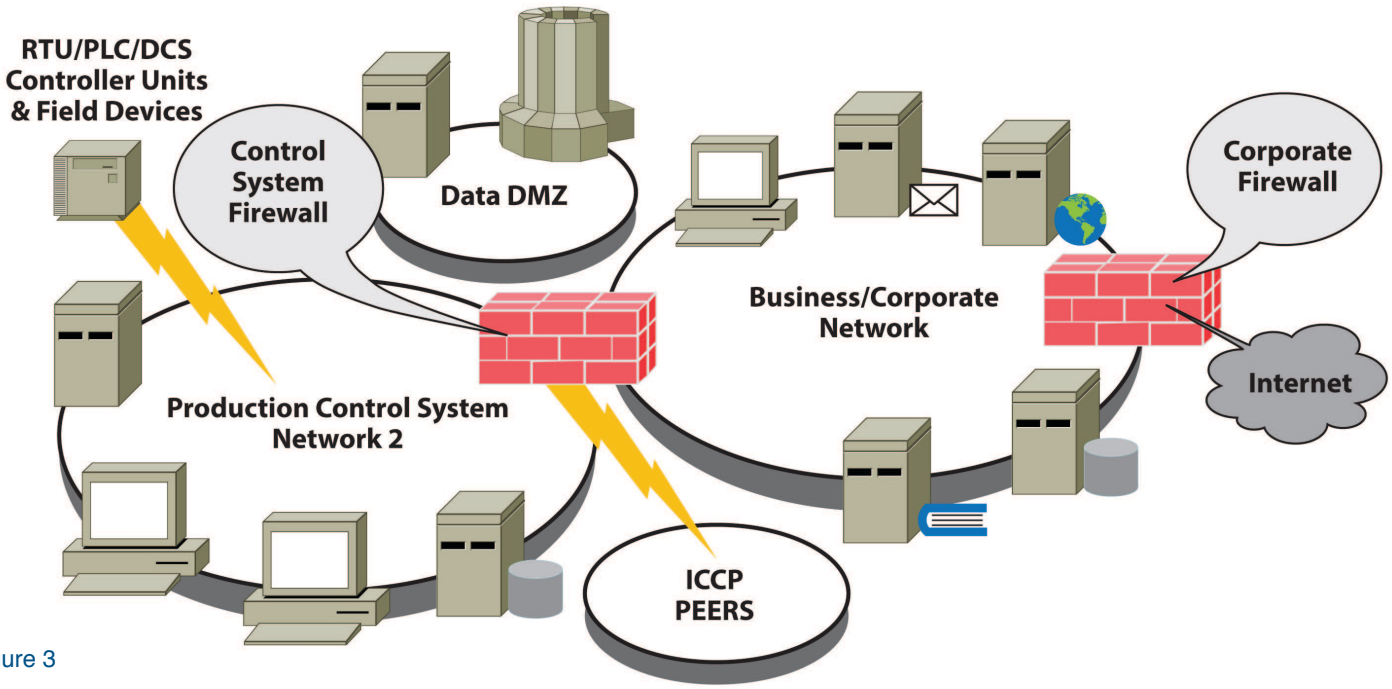


Figure 3

The critical aspect of a DMZ is to control the flow of communications between each of the network segments for which the DMZ provides segregation. This is typically done through specially configured firewalls or routers, which enforce controlled access to/from the DMZ, and can deny all other nonauthorized traffic. The best rule set configurations do not allow the zones to bypass the DMZ; instead they force traffic to use the systems within the DMZ to push, pull or present data. The DMZ should restrict communication flows to the most restrictive set of IPs, ports and protocols, thereby providing an additional boundary or layer or defense from potential compromise.

When configured correctly, networks segmented by DMZs are much harder to compromise. An attacker with the aim of accessing a control system must first gain access through a business network's perimeter firewall, then find a system that is authorized to communicate with a host resident within the boundary DMZ. Where the DMZ is configured with the most restrictive communications paths, an attacker may be effectively thwarted at this point as traffic rules enforced may not allow communication from a host within the boundary DMZ to the business network. Even if the business network becomes compromised, the DMZ isolating the control systems will provide another layer of defense in preventing access to your control system network.

ICS-CERT is continuously working closely with the control systems community to increase awareness of defense-in-depth strategies for cybersecurity. In the next Monitor, we will discuss other common vulnerabilities and provide further information on how to mitigate them and strengthen your overall security posture.

### REGISTER NOW FOR THE ICSJWG SPRING MEETING

The Industrial Control Systems Joint Working Group (ICSJWG) will be held at the Indiana Government Center South, 302 W. Washington St, Indianapolis, Indiana, USA, from June 3−5, 2014. The 2014 Spring ICSJWG Meeting will bring together asset owners and operators, government professionals, vendors, systems integrators and academic professionals to discuss the latest initiatives impacting security of ICSs and interact with colleagues and peers addressing the risk of threats and vulnerabilities to their systems.

The goal of this meeting is to provide a venue where participants can obtain current information, research findings and practical tools to enhance the security and resilience of industrial control systems. At the June meeting, participants will prioritize strategies for establishing, maintaining and expanding stakeholder collaboration and activities that facilitate communication among agencies and sectors, and strengthen the public-private partnerships the ICS community.

The meeting will include 3 days of presentations and discussions about ICS security. These 3 days will include keynote speakers, practical demonstrations, plenary sessions, panel presentations and both classified and unclassified briefings.

Register for the meeting by sending a registration request to ICSJWG.Communications@hq.dhs.gov. Include your name and company along with your Sector affiliation(s) and Role(s) with your request. Please register by May 12, 2014.

## ENHANCED CYBERSECURITY SERVICES (ECS) PROGRAM

In February 2014, a year after President Obama issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity – the White House released a new Cybersecurity Framework, a set of guidelines to help the private sector enhance cybersecurity and address cyber threats and vulnerabilities.

To help the private sector learn about and adopt the Framework, the Department of Homeland Security (DHS) created and launched the Critical Infrastructure Cyber Community (C3) Voluntary Program, which gives critical infrastructure owners and operators access to services and cybersecurity experts in the DHS. These experts have knowledge about specific emerging cyber threats ways to counter those threats, and guidance for mitigating cyber vulnerabilities facing critical infrastructure.

One service DHS offers is the voluntary Enhanced Cybersecurity Services (ECS) program. This program helps critical infrastructure entities protect themselves against cyber threats to the systems upon which so many Americans rely. This program is a good example of information sharing with confidentiality, privacy and civil liberties protections built into its structure.

**Building on the Foundation**

The Office of Cybersecurity & Communications (CS&C) has established a community of trust between the public and private sectors in order to improve the Nation's overall computer network defense posture. Through sharing cyber threat information with its partners, DHS enables the detection, prevention and mitigation of threats. This builds a holistic understanding of cyber threat activity occurring across the 16 Critical Infrastructure sectors and the federal government.

The ECS program is a significant component of CS&C's information sharing strategy. It builds on existing partnerships by establishing a voluntary information-sharing program that helps critical infrastructure owners and operators improve protection of their systems from unauthorized access, exploitation, or data exfiltration.

The ECS program has established processes and security requirements so that DHS can securely share sensitive and classified cyber threat information to appropriately cleared private sector cybersecurity Commercial Service Providers (CSP). Access to this kind of information will enable CSPs to offer better security services, which will augment the existing services they provide their customers.

As with other DHS information-sharing programs, participation in ECS is voluntary and designed to protect government intelligence, corporate information security and the privacy of participants while enhancing the security of critical infrastructure.

**How does this work?**

The ECS program works with cybersecurity organizations from across the U.S. Government to access a broad range of cyber threat information. DHS analyzes information that is specific to identifying known or suspected cyber threats in the form of "indicators," which are human-readable cyber data used to identify malicious cyber activity.

The indicators range in classification from unclassified to Top Secret/SCI. Classification of identified indicators is dictated by its source. CS&C identifies and validates the indicators that are critical for protecting critical infrastructure and then shares the indicators with participating Commercial Service Providers that will only use them to provide approved ECS for their critical infrastructure customers. These can be used to create "signatures" that are machine readable and able to detect patterns of network traffic that negatively affect critical infrastructure systems. ECS are intended to augment, not replace, existing cybersecurity services operated by or available to critical infrastructure entities.

Critical infrastructure customers do not receive threat information directly from the government, but through their pre-approved CSP, as shown in Figure 5.

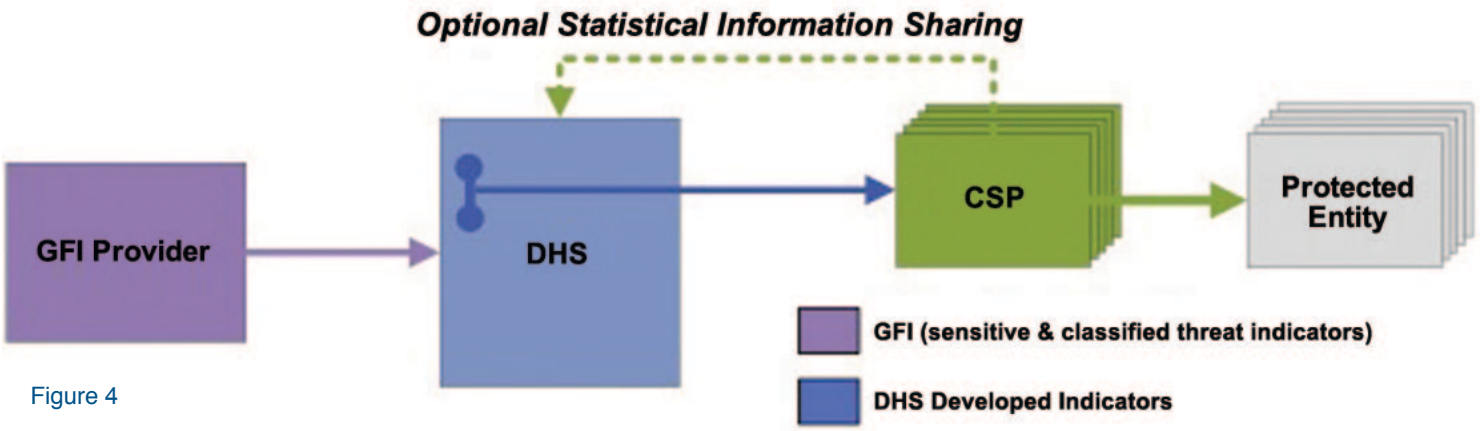


Figure 4

**What about Privacy?**

Protecting our citizens' privacy and civil liberties is a top priority for the administration and the department. In fact, the ECS program was built with these protections in mind.

ECS does not allow government monitoring of private communications. CSPs may voluntarily share limited statistical information, such as the timestamp of the cyber event, indicator that was involved, and the identification of the critical infrastructure sector of which the affected company is a member. Under the ECS program, ECS-related information is not directly shared between customers of the CSPs and the government.

Information, such as the company name or other identifiable information, is not shared. CS&C will share the statistical information it receives under ECS consistent with its existing policies and procedures, including with other U.S. government entities with cybersecurity responsibilities.

Click here to read more about the ECS program Privacy Impact Assessment.

## Program Participants

**Commercial Service Providers (CSPs) / Operational Implementers (OIs)**

In order to participate in the ECS program and provide ECS, CSPs and OIs must meet the eligibility requirements set forth by the ECS program and its partners. CSPs and OIs are responsible for handling, using and maintaining all classified and sensitive government furnished information in accordance with the defined security requirements set forth by the ECS program. Once vetted, CSPs and OIs will enter into a Memorandum of Agreement (MOA) with DHS, and then complete the security accreditation process in order to participate in the program and receive government-furnished threat indicators. CSPs may only deliver ECS to DHS-validated critical infrastructure entities. The CSPs may also use the services to protect themselves.

To date, two participating CSPs are fully approved to provide ECS. Interested Critical Infrastructure entities may contact one of the below for additional information:

- AT&T (ecs-pmo@list.att.com)
- CenturyLink (ecs@centurylink.com)

For more information please refer to the ECS Program web page at: http://www.dhs.gov/enhanced-cybersecurity-services

## Critical Infrastructure (CI) Entities

**Current Participation**

As of February 2014, there are 40 participants within the ECS Program covering three sectors plus federal government entities.

1. Communications Sector
2. Defense Industrial Base (DIB) Sector
3. Energy Sector
4. Federal Government

In addition, 13 companies are validated and working with the CSPs to begin participating within the ECS Program covering five sectors.

1. Financial Sector
2. Defense Industrial Base (DIB) Sector
3. Energy Sector
4. Chemical Sector
5. Information Technology Sector

1. OIs may utilize the ECS to only protect their own internal network

## ACTIONABLE INFORMATION THROUGH STIX

Providing actionable information that is quickly digestible and useful to critical infrastructure owners, operators and vendors has led to the adoption of the STIX (Structured Threat Information eXpression) format. ICS-CERT has begun distributing alerts, advisories and bulletins in a STIX-compliant format, which includes both informational and actionable indicators. STIX is a DHS-sponsored and community-driven effort to define and develop a standardized language to represent cyber threat information. The overall goal of STIX is to make intelligence, indicators and cyber data machine-readable in a standard format.

At the core, STIX provides architecture for integrating a diverse set of cyber threat information encompassing:

- Cyber observables (network or host-based indicators and artifacts),
- Indicators (observables correlated with additional contextual information),
- Incidents (instances of specific adversarial actions),
- TTPs (tactics, techniques and procedures – attack patterns, malware, exploits, etc.),
- Exploit targets (vulnerabilities, weaknesses or configurations),
- Courses of action (best practices, defensive actions, remediation),
- Cyberattack campaigns (collection of Incidents and/or TTPs demonstrating a shared intent) and
- Cyberthreat actor (characterization of the adversary).

**So What Does This Mean?**

As ICS-CERT releases STIX-compliant XML artifacts to accompany our alerts and advisories, an organization can simply download the machine-readable XML files and parse or ingest them into a third-party (or custom built) application that supports the XML framework. This structure empowers organizations to readily enhance their detection and protection capabilities by automatically incorporating indicators and actionable information within the context of their existing security platforms and architecture.

**Automation**

Automated ingestion of STIX-based artifacts allows asset owners and operators to reduce/eliminate the overhead of manually incorporating observables and indicators into their existing detection toolsets, while increasing the amount of contextual information available to assist analysts in assessing the impact and priority of these indicators. Streamlining this process should reduce the time from incident detection to containment with the ultimate goal being detection and prevention. DHS has launched the initial phase of TAXII (Trusted Automation eXchange of Indicator Information) data delivery services to enable an automated exchange of information represented using the STIX language.

For additional information pertaining to STIX and TAXII, please contact ICS-CERT.

## WEB-BASED TRAINING IS NOW AVAILABLE

ICS-CERT is pleased to announce the launch of the web-based training Cybersecurity for Industrial Control Systems (210W). This course is an online version of our 101 and 201 instructor-led courses. The course contains modules covering many aspects of cybersecurity for industrial control systems.

This course serves as an introduction to the basics of industrial control systems security. The instruction includes a comparative analysis of IT and control system architecture, security vulnerabilities and mitigation strategies unique to the control system domain.

Students will receive technical instruction on the protection of industrial control systems using offensive and defensive methods. At the conclusion of the course students will understand how cyber attacks could be launched, why they work and mitigation strategies to increase the cybersecurity posture of their control system.

You may view this web-based training at: https://ics-cert-training.inl.gov/.

## DOCUMENT FAQ

### What is the publication schedule for this digest?

ICS-CERT publishes the ICS-CERT Monitor when an adequate amount of pertinent information has been collected.

ICS-CERT provides this newsletter as a service to personnel actively engaged in the protection of critical infrastructure assets. The public can view this document on the ICS-CERT Web page at: http://www.us-cert.gov/control_systems/ics-cert/.

Please direct all questions or comments about the content, or suggestions for future content, to ICS-CERT at: ics-cert@hq.dhs.gov.

## RECENT PRODUCT RELEASES

### ALERTS

ICS-ALERT-14-015-01 Ecava IntegraXor Buffer Overflow Vulnerability, 01/15/2014

### ADVISORIES

ICSA-14-087-01 Siemens ROS Improper Input Validation, 03/28/2014

ICSA-14-086-01 Schneider Electric Serial Modbus Driver Buffer Overflow, 03/27/2014

ICSA-14-079-01 Siemens SIMATIC S7-1200 Improper Input Validation Vulnerabilities, 03/20/2014

ICSA-14-079-02 Siemens SIMATIC S7-1200 Vulnerabilities, 03/20/2014

ICSA-14-051-03A Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability (Update A), 03/18/2014

ICSA-12-213-01A Sielco Sistemi Winlog Multiple Vulnerabilities (Update A), 03/18/2014

ICSA-14-073-01 Siemens SIMATIC S7-1500 CPU Firmware Vulnerabilities, 03/14/2014

ICSA-14-072-01 Schneider Electric StruxureWare SCADA Expert ClearSCADA Parsing Vulnerability, 03/13/2014

ICSA-14-070-01 Yokogawa CENTUM CS 3000 Vulnerabilities, 03/11/2014

ICSA-14-058-01 Schneider Electric Floating License Manager Vulnerability, 02/27/2014

ICSA-14-058-02 Schneider Electric OFS Buffer Overflow Vulnerability, 02/27/2014

ICSA-13-350-01A Schneider Electric CitectSCADA Products Exception Handler Vulnerability (Update A), 02/26/2014

ICSA-14-051-01 ICONICS GENESIS32 Insecure ActiveX Control, 02/20/2014

ICSA-14-051-02 Mitsubishi Electric Automation MC-WorX Suite Unsecure ActiveX Control, 02/20/2014

ICSA-14-051-04 NTP Reflection Attack, 02/20/2014

ICSA-14-010-01 MatrikonOPC Improper Input Validation, 02/11/2014

ICSA-14-035-01 Siemens SIMATIC WinCC OA Multiple Vulnerabilities, 02/04/2014

ICSA-14-021-01 Rockwell RSLogix 5000 Password Vulnerability, 02/04/2014

ICSA-14-030-01 3S CoDeSys Runtime Toolkit NULL Pointer Dereference, 01/30/2014

ICSA-14-006-01 Schneider Electric Telvent SAGE RTU DNP3 Improper Input Validation Vulnerability, 01/30/2014

ICSA-14-023-01 GE Proficy Vulnerabilities, 01/23/2014

ICSA-14-016-01 Ecava IntegraXor Buffer Overflow Vulnerability, 01/16/2014

ICSA-13-344-01 WellinTech Vulnerabilities, 01/14/2014

ICSA-14-007-01A Sierra Wireless AirLink Raven X EV-DO Vulnerabilities (Update A), 01/14/2014

ICSA-14-014-01 Schneider Electric ClearSCADA Uncontrolled Resource Consumption Vulnerability, 01/14/2014

ICSA-14-008-01 Ecava Sdn Bhd IntegraXor Project Directory Information Disclosure Vulnerability, 01/08/2014

ICSA-11-094-02B Advantech/Broadwin WebAccess RPC Vulnerability (Update B), 01/07/2014

### OTHER

October/November/December 2013–ICS-CERT Monitor

Follow ICS-CERT on Twitter: @icscert

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS

**GPS Pioneer Warns on Network's Security**
2014-02-14

The Global Positioning System helps power everything from in-car satnavs and smart bombs to bank security and flight control, but its founder has warned that it is more vulnerable to sabotage or disruption than ever before – and politicians and security chiefs are ignoring the risk.

Impairment of the system by hostile foreign governments, cyber criminals – or even regular citizens – has become "a matter of national security", according to Colonel Bradford Parkinson, who is hailed as the architect of modern navigation.
http://www.cnbc.com/id/101417376

**Abusing Cloud Services for Cybercrime**
2014-02-14

Building a botnet typically involves infecting a PC. But at the upcoming RSA Conference , two researchers plan to show how to build one with free cloud services. Bishop Fox security researchers Oscar Salazar and Rob Ragan were able to automate the process of signing up for accounts on various cloud services, opening the door for abuse of legitimate cloud infrastructure in the name of cybercrime. It is not the first time that researchers have discussed the use of cloud platforms by attackers. Recent research from Solutionary for example showed that cybercriminals are increasingly using legitimate hosting providers like Amazon and GoDaddy to host malicious domains.
http://www.darkreading.com/attacks-breaches/abusing-cloud-services-for-cybercrime/240166135

**White House Pushes Cybersecurity Framework for Critical Infrastructure**
2014-02-12

A new cybersecurity framework released Wednesday by U.S. President Barack Obama's administration aims to help operators of critical infrastructure develop comprehensive cybersecurity programs.

The voluntary framework creates a consensus on what a good cybersecurity program looks like, senior administration officials said. The 41-page framework takes a risk management approach that allows organizations to adapt to "a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner," according to the document.
http://www.pcworld.com/article/2097320/white-house-pushes-cybersecurity-framework-for-critical-infrastructure.html
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf

**FIS Joins Forces with Microsoft to Advance Cybersecurity**
2014-02-12

Underscoring its commitment to deliver information security excellence, FIS(TM) (NYSE: FIS), the world's largest provider of banking and payments technology, announces its selection by Microsoft as a partner in the fight against cybercrime.

Under the agreement, FIS representatives will work hand-in-hand with forensic analysts, software developers and researchers at the Microsoft Cybercrime Center, which opened in November 2013. The partnership goal is to increase cooperative action between international law enforcement and private industry in order to help continuously improve the security of payments and financial transactions worldwide and make the Internet a safer place to do business.
http://online.wsj.com/article/PR-CO-20140212-916877.html

**One Agency Should Have Authority to Deal With Power Grid Threats: FERC Chief**
2014-02-12

Congress should consider passing legislation that would give one agency "clear and direct authority" to respond to imminent threats to the US power system, Cheryl LaFleur, acting chairman of the Federal Energy Regulatory Commission has told lawmakers.

"This authority should include the ability to require action before a physical or cyber national security incident has occurred," LaFleur said in a Tuesday letter. Any new authority, she said, should not impede FERC's existing authority to work with the North American Electric Reliability Corp. to set reliability standards for the grid, a process that can often take months to complete.
http://www.platts.com/latest-news/electric-power/washington/one-agency-should-have-authority-to-deal-with-21208788

**Govt report: Cyberattacks Not Coordinated**
2014-02-10

A multi-agency government task force looking into cyberattacks against retailers says it has not come across evidence suggesting the attacks are a coordinated campaign to adversely affect the U.S. economy.

In a two-page report, the National Cyber Investigative Joint Task Force says the global implications of the retail attacks and the economic impact to private business and individual citizens cannot be overstated.
http://www.ktvn.com/story/24686584/govt-report-cyberattacks-not-coordinated

http://stream.wsj.com/story/latest-headlines/SS-2-63399/SS-2-450942/

**OIG to Review Medical Device Security**
2014-02-10

The HHS Office of Inspector General plans to scrutinize a number of security-related activities in the healthcare sector in fiscal 2014, including reviewing whether hospitals' security controls over networked medical devices are sufficient to effectively protect patients' information.
http://www.govinfosecurity.com/oig-to-review-medical-device-security-a-6490

**Study: Pentagon Fuel Supply at Risk of Hack**
2014-02-07

The Pentagon should take a page from the Department of Homeland Security's cyber defense playbook for energy infrastructure to guard against electronic assault on its fuel supply chain, according to a new study.

The Defense Department's use of unsecured networks to oversee the distribution of fuel and other logistical activities has left it vulnerable to the same kind of malware-based cyberattack that crippled 30,000 computers in oil giant Saudi Aramco's networks in 2012, according to "Hacks on Gas: Energy, Cybersecurity and U.S. Defense," a report written by Christopher Bronk, a fellow in IT policy at Rice University's Baker Institute. He produced the report for the U.S. Army War College's Strategic Studies Institute.
http://fcw.com/articles/2014/02/07/pentagon-fuel-supply-at-risk-of-hack.aspx
http://bakerinstitute.org/media/files/Research/e00e5348/Pub-IT-HacksonGas-020514.pdf

**Study: Most Security Pros Unsure Whether They Could Handle A Breach**
2014-02-13

A survey conducted by the Ponemon Institute and sponsored by security company AccessData reports that many security pros are worried that they would not know the root cause of a breach, or that they would be able to prioritize their responses. "When a CEO and board of directors asks a security team for a briefing immediately following an incident, 65 percent of respondents believe that the briefing would be purposefully modified, filtered or watered down" because of a lack of information, the study says. "Additionally, 78 percent of respondents believe most CISOs would make a 'best effort guess' based on limited information, and they would also take action prematurely and report that the problem had been resolved without this actually being the case."
http://www.darkreading.com/management/study-most-security-pros-unsure-whether/240166084

**'The Mask' Cyber Spying Operation Targets Government Agencies**
2014-02-11

Security researchers have uncovered a cyber-espionage campaign called Careto, or The Mask, that has been targeting government agencies, energy companies and activists in 31 countries for seven years. The campaign, which appears to have been authored by Spanish attackers, is one of the most advanced global cyber-espionage operations to date, according to Kaspersky Lab's security research team. http://www.telegraph.co.uk/technology/internet-security/10630272/The-Mask-cyber-spying-operation-targets-government-agencies.html

**Cyber Contest Hones Military Cadets' Skills**
2014-02-06

The U.S. Defense Department launched a new competition to promote cybersecurity education and training in the nation's military service academies. Beginning last November, the three service academies created teams to compete in the Service Academy Cyber Stakes, which culminated in a major interschool event held over the weekend of February 1-2 at the Carnegie Mellon campus in Pittsburgh.

For some years, the Defense Department has been working to increase the number of cybersecurity personnel. One major goal is to have some 4,000 specialists trained by 2017. To get the number and quality of cyber experts needed, the Defense Department has focused on training and educating—especially for future officers who will be charged with defending national cyber assets.
http://www.afcea.org/content/?q=node/12300

**Critical Infrastructure Cyber Bill Moves Forward**
2014-02-05

The latest round of cybersecurity legislation is moving ahead in the House, with the Homeland Security Committee on Feb. 5 approving a bill by voice vote that seeks to protect critical infrastructure and codify information-sharing practices. According to a summary of the bill, the measure would formalize numerous existing government cybersecurity efforts, such as information-sharing initiatives between the public and private sectors and assessments of the cyber workforce. It would also strengthen the National Cybersecurity and Communications Integration Center and prohibit new regulatory authorities at agencies, particularly the Department of Homeland Security.
http://fcw.com/articles/2014/02/05/critical-infrastructure-cyber-bill-moves-forward.aspx

**Cyberattacks are on the Rise. And Health-Care Data is the Biggest Target.**
2014-02-05

The recent spate of cyberattacks on retailers has scared shoppers and triggered debates on Capitol Hill about whether consumers' data is being properly protected. Despite its security flaws, the retail sector isn't the one most vulnerable to breaches. That dubious honor goes to health care.
http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/05/cyberattacks-are-on-the-rise-and-health-care-data-is-the-biggest-target/

**DHS Revs Up its Part of the Cyber Executive Order**
2014-01-31

"We will be launching what we call the voluntary program on Feb. 14, enabling companies of all sizes to follow some basic cybersecurity policies and due care that have been designed through the framework by the best scientists in the private sector and the government that we have. [We are] looking at how we can incentivize companies, again of all sizes, to be more secure, to enable big companies to share their best practices, to drive markets for small to medium to enable economies of scale for companies that are smaller and may not be able to afford to now have very good cybersecurity, [and] to have a cybersecurity policy," said Phyllis Schneck, the deputy undersecretary for cybersecurity at NPPD, in an exclusive interview with Federal News Radio.
http://www.federalnewsradio.com/?nid=473&sid=3553526

**Emergency Services Like 911 No Longer Cyber-safe, GAO Reports**
2014-01-30

Federal and state emergency services like 911 are no long safe from cyberattacks or cybersecurity privacy breaches, according to a report released Tuesday from the Government Accountability Office.
http://dailycaller.com/2014/01/30/emergency-services-like-911-no-longer-cyber-safe-gao-reports/
http://www.gao.gov/products/GAO-14-125

**Air Force Researchers Plant Rootkit In A PLC**
2014-01-27

Researchers with the U.S. Air Force Institute of Technology (AFIT) have created a prototype rootkit that can sit undetected in the firmware of a programmable logic controller (PLC) device and corrupt utility and plant floor operations.

PLCs -- which run various industrial processes from spinning centrifuges of uranium to operating amusement park rides -- traditionally have not been built with security in mind, and little if any technology exists to track or detect rogue code running on them.
http://www.darkreading.com/attacks-breaches/air-force-researchers-plant-rootkit-on-a/240165715

**Electric Utility Cybersecurity Regulations have a Serial Problem**
2014-01-24

A class of SCADA vulnerabilities discussed at a recent conference is getting attention not only for the risks they pose to master control systems at electric utilities, but also for illuminating a dangerous gap in important critical infrastructure regulations.

"Where serial lines come into a master station, for instance, they won't have the same level of protection that a TCP/IP-based connection would have," said Michael Toecker, an ICS security consultant and engineer at Digital Bond. "There's a complete regulatory blind spot there in the current version of the NERC standards."
http://threatpost.com/electric-utility-cybersecurity-regulations-have-a-serial-problem/103838

**Machine Resiliency as a Defense**
2014-01-21

In 2014, the PC you unbox and provision on your network is likely to be a better machine, better able to withstand attack, more resilient than a PC of just a few years ago.

Those improvements are the result of efforts and investments in security assurance from OSVs, ISVs, OEMs and hardware suppliers. Let's take BIOS, for example. BIOS isn't often fodder for headlines, but it matters. BIOS is the low level firmware that controls machine operations before the OS takes control. Even less visible is the BIOS's contribution to system security in testing, verifying and authenticating the hardware to ensure it has not been compromised.
http://www.darkreading.com/threat-intelligence/machine-resiliency-as-a-defense/240165535

**Warning Computer Hackers Shortens Their Intrusion**
2014-01-17

University of Maryland researchers now are exploring the conduct of the computer intruders. In a groundbreaking new study, they show for the first time that the appearance of a warning banner

upon entry significantly shortens the time an intruder remains on an attacked system. The researchers also found that slow network speed combined with a warning message further hastens criminal hackers' departure from the system.
http://phys.org/news/2014-01-hackers-shortens-intrusion.html

**Proofpoint Uncovers Internet of Things (IoT) Cyberattack**
2014-01-16

Proofpoint, Inc., a leading security-as-a-service provider, has uncovered what may be the first proven Internet of Things (IoT)-based cyberattack involving conventional household "smart" appliances. The global attack campaign involved more than 750,000 malicious email communications coming from more than 100,000 everyday consumer gadgets such as home-networking routers, connected multi-media centers, televisions and at least one refrigerator that had been compromised and used as a platform to launch attacks.
http://online.wsj.com/article/PR-CO-20140116-910437.html

**New UMich Formula Predicts Perfect Moment For Hackers To Strike**
2014-01-15

The timing of a cyber-attack is crucial to overcoming measures designed to defend or repel the attacks and a new study from researchers at the University of Michigan has revealed a mathematical model that could be used to optimize the timing of would-be hackers.

In the study, which was published in the Proceedings of the National Academy of Sciences (PNAS), the research team said nations around the world are cataloging defects in Internet security systems not already identified by someone else – also known as "zero-day exploits." The researchers focused their model on identifying the precise time to take advantage of the flaws.
http://www.redorbit.com/news/technology/1113047352/cyber-attack-prediction-system-umich-011514/

**Cyber Command Funding More than Doubles**
2014-01-14

The House approved a short-term federal spending bill on Tuesday to allow time for the expected passage of a fiscal 2014 spending package that includes $447 million for the Pentagon component that launches cyber weapons and deflects hacks against civilian and military networks. That's more than a two-fold increase over Cyber Command's fiscal 2013 budget of $191 million.
http://www.nextgov.com/defense/2014/01/cyber-command-funding-more-doubles/76859/

**Defense Leaders Say Cyber is Top Terror Threat**
2014-01-06

Defense officials see cyberattacks as the greatest threat to U.S. national security, according to a survey released Monday.

Forty-five percent of respondents to the Defense News Leadership

Poll named a cyberattack as the single greatest threat—nearly 20 percentage points above terrorism, which ranked second.

The Defense News Leadership Poll, underwritten by United Technologies, surveyed 352 Defense News subscribers, based on job seniority, between Nov. 14 and Nov. 28, 2013. The poll targeted senior employees within the White House, Pentagon, Congress, and the defense industry.
http://www.nationaljournal.com/defense/defense-leaders-say-cyber-is-top-terror-threat-20140106

**Converging Physical and Cybersecurity**
2013-12-19

President Barack Obama's Executive Order on Improving Critical Infrastructure Cybersecurity and his Presidential Policy Directive on Critical Infrastructure Security and Resilience are two of the first official acknowledgments of the inextricable link between physical and cybersecurity.

The directives empower federal organizations to embrace holistic security measures to protect our nation's critical infrastructure, buildings, assets, information and people. In order to achieve a truly holistic approach, federal organizations must close the schism between physical and cybersecurity divisions.
http://fcw.com/articles/2013/12/19/drilldown-converging-physical-and-cybersecurity.aspx

**House Homeland Security Leaders Introduce Cybersecurity Legislation**
2013-12-16

Dec. 11 --Leaders of the House Homeland Security Committee Dec. 11 introduced a bipartisan bill (H.R. 3696) to address cyberattacks on the nation's banking system, energy pipelines, telecommunications networks and other "critical infrastructure."

H.R. 3696 would amend the Homeland Security Act, 6 U.S.C. § 101, to clarify and expand its scope to cover cybersecurity issues.
http://www.bna.com/house-homeland-security-n17179880741/

**Cyberspace warriors graduate with Army's newest military occupational specialty**
2013-12-06

Fifteen Soldiers made history when they were awarded the newest Army military occupational specialty, 25D, cyber network

## OPEN SOURCE SITUATIONAL AWARENESS HIGHLIGHTS - Continued

defender, during a graduation ceremony Nov. 27, held in Alexander Hall at Fort Gordon, Ga.
Soldiers completed a 14-week course, considered rigorous for its curriculum, to learn the skills needed to meet the demand for cyber warfare.
http://www.army.mil/article/116564/
http://defensesystems.com/articles/2013/12/09/army-cyber-network-defender-graduation.aspx

**NATO Launches 'Largest Ever' Cyber-Security Exercises**
2013-11-26

NATO has kicked off Cyber Coalition 2013, the largest ever exercise of its kind intended to thwart massive, simultaneous attacks on member states and their allies. The three-day exercise, based at the 27 member alliance's cyber defense center in Estonia, will include participants from over 30 European states.

"With around 100 participants in Tartu [Estonia] and over 300 in national capitals from 32 nations, Cyber Coalition 2013 is the largest exercise of its kind in terms of participating countries," NATO said in a statement.
http://rt.com/news/nato-cyber-exercises-estonia-344/

## UPCOMING EVENTS

### June

**Industrial Control Systems Cybersecurity (301) Training (5 days)**
**International Partners**

**CLOSED**

June 9–13, 2014
Idaho Falls, Idaho, USA

### July

**Industrial Control Systems Cybersecurity (301) Training (5 days)**
**North American Partners**

**CLOSED**

July 14–18, 2014
Idaho Falls, Idaho, USA

### September

**Industrial Control Systems Cybersecurity (301) Training (5 days)**
**North American Partners**

September 8–12, 2014
Idaho Falls, Idaho, USA

*Course Description and Registration*
(will be available in mid-June)

## COORDINATED VULNERABILITY DISCLOSURE

ICS-CERT actively encourages researchers and ICS vendors to use a coordinated vulnerability disclosure process when possible. Ideally, this coordinated disclosure process allows time for a vendor to develop and release patches, and for users to test and deploy patches prior to public vulnerability disclosure. While this process is not always followed for a variety of reasons, ICS-CERT continues to promote this as a desirable goal.

Bridging the communication gap between researchers and vendors, as well as coordinating with our CERT/CC and US-CERT partners, has yielded excellent results for both the researchers and vendors. To learn more about working with ICS-CERT in this coordinated disclosure process, please contact ICS-CERT at ics-cert@hq.dhs.gov or toll free at 1-877-776-7585.

## COORDINATED VULNERABILITY DISCLOSURE - Continued

**RESEARCHERS ASSISTING ICS-CERT WITH PRODUCTS THAT WERE PUBLISHED JANUARY/FEBRUARY/MARCH**

ICS-CERT appreciates having worked with the following researchers:

- Researcher Aivar Liimets from Martem Telecontrol Systems, ICSA-14-087-01 Siemens ROS Improper Input Validation, 3/28/2014.
- Carsten Eiram of Risk-Based Security, ICSA-14-086-01 Schneider Electric Serial Modbus Driver Buffer Overflow, 3/27/2014.
- Ralf Spenneberg of OpenSource Training, Lucian Cojocar of EURECOM, Sascha Zinke from the FU Berlin's work team SCADACS, and Positive Technologies' researchers (Alexey Osipov, and Alex Timorin), ICSA-14-079-02 Siemens SIMATIC S7-1200 Vulnerabilities, 3/20/2014.
- Researchers Ling Toh Koh, Ng Yi Teng, Seyed Dawood Sajjadi Torshizi, Ryan Lee, and Ho Ping Hou of EV-Dynamic, Malaysia, ICSA-14-051-03A Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability (Update A), 3/18/2014.
- Researchers Carlos Mario Penagos Hollmann of IOActive, Michael Messner, and Luigi Auriemma, ICSA-12-213-01A Sielco Sistemi Winlog Multiple Vulnerabilities (Update A), 3/18/2014.
- Positive Technology researchers (Yury Goltsev, Llya Karpov, Alexey Osipov, Dmitry Serebryannikov and Alex Timorin), ICSA-14-073-01 Siemens SIMATIC S7-1500 CPU Firmware Vulnerabilities, 3/14/2014.
- J Andrew Brooks identified and reported to The Zero Day Initiative (ZDI), ICSA-14-072-01 Schneider Electric StruxureWare SCADA Expert ClearSCADA Parsing Vulnerability, 3/13/2014.
- Juan Vazquez of Rapid7 Inc., and independent researcher Julian Vilas Diaz, ICSA-13-350-01A Yokogawa CENTUM CS 3000 Vulnerabilities, 3/11/2014.
- Independent researcher (known as) 0x7A240E67, ICSA-14-058-02 Schneider Electric OFS Buffer Overflow Vulnerability, 2/27/2014.
- Researcher Carsten Eiram of Risk Based Security, ICSA-13-350-01A Schneider Electric CitectSCADA Products Exception Handler Vulnerability, 2/26/2014.
- The anonymous researcher, "Blake," ICSA-14-051-02 Mitsubishi Electric Automation, Inc. MC-WorX Suite Insecure ActiveX Control, 2/20/2014.
- Researchers Ling Toh Koh, Ng Yi Teng, Seyed Dawood Sajjadi Torshizi, Ryan Lee, and Ho Ping Hou of EV-Dynamic, ICSA-14-051-03 Siemens RuggedCom Uncontrolled Resource Consumption Vulnerability, 2/20/2014.
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-14-010-01 MatrikonOPC Improper Input Validation, 02/11/2014
- Researchers Gleb Gritsai, Ilya Karpov, and Kirill Nesterov of Positive Technologies, ICSA-14-035-01
- Siemens SIMATIC WinCC OA Multiple Vulnerabilities, 02/04/2014
- Independent researcher Stephen Dunlap, ICSA-14-021-01 Rockwell RSLogix 5000 Password Vulnerability, 02/04/2014
- Independent researcher Nicholas Miles, ICSA-14-030-01 3S CoDeSys Runtime Toolkit NULL Pointer Dereference, 01/30/2014
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-14-006-01 Schneider Electric Telvent SAGE RTU DNP3 Improper Input Validation Vulnerability, 01/30/2014
- Researchers amisto0x07 and Z0mb1E of Zero Day Initiative, ICSA-14-023-01 GE Proficy Vulnerabilities, 01/23/2014
- Independent researcher Luigi Auriemma, ICSA-14-016-01 Ecava IntegraXor Buffer Overflow Vulnerability, 01/16/2014
- Zero Day Initiative, ICSA-13-344-01 WellinTech Vulnerabilities, 01/14/2014
- Cimation, ICSA-14-007-01A Sierra Wireless AirLink Raven X EV-DO Vulnerabilities (Update A), 01/14/2014
- Adam Crain of Automatak and independent researcher Chris Sistrunk, ICSA-14-014-01 Schneider Electric ClearSCADA Uncontrolled Resource Consumption Vulnerability, 01/14/2014
- Zero Day Initiative, ICSA-14-008-01 Ecava Sdn Bhd IntegraXor Project Directory Information Disclosure Vulnerability, 01/08/2014
- Independent researcher Rubén Santamarta, ICSA-11-094-02B Advantech/Broadwin WebAccess RPC Vulnerability (Update B), 01/07/2014

## RESEARCHERS CURRENTLY WORKING WITH ICS-CERT

ICS-CERT appreciates the following researchers who continue to work with us to resolve exploits:

Aaron Patterson
Aaron Portnoy
Adam Crain
Aivar Liimets
Alex Timorin
Alexey Osipov
Amisto0x07
Andrew Brooks
Anton Popov
Artem Chaykin
Arthur Gervais
Billy Rios
"Blake"
Bob Radvanovsky
Brendan Harris
Brian Meixell
Carlos Mario Penagos Hollmann
Carsten Eiram
Cesar Cerrudo
Christopher Scheuring
Christopher Sistrunk
Dale Peterson
Dillion Beresford
Dmitry Serebryannikov
Eireann Leverett
Eric Forner`
Eric Wustrow
Gleb Gritsai
Hisashi Kojima
Ho Ping Hou
Ilya Karpov
J. Alex Halderman
J Andrew Brooks
Joel Langill
John Adam Crain
Jon Christmas
Juan Vasquez
Jürgen Bilberger
Kirill Nesterov
Kuang-Chun Hung (ICST)
Kyle Stone
Ling Toh Koh
Llya Karpov
Lucas Apa
Lucian Cojocar
Luigi Auriemma
Marc Ayala
Mashahiro Nakada
Mehdi Sabraoui
Michael Messner
Michael Toecker
Nadia Heninger
Neil Smith
Ng Yi Teng
Nicholas Miles
Nin3
Postive Technologies Security
Ralf Spenneberg
Reid Wightman
Roman Ilin
Rubén Santamarta
Ryan Green
Ryan Lee
Sascha Zinke
Sergey Bobrov
Sergey Gordeychick
Seyed Dawood Sajjadi Torshizi
Shawn Merdinger
Stephen Dunlap
Terry McCorkle
Timur Yunusov
Wei Gao
Yury Goltsev
Zakir Durumeric
Z0mb1E
0x7A240E67

## We Want To Hear From You

A key aspect of our mission is providing relevant and timely cybersecurity information products and services to industrial control system (ICS) stakeholders. As we develop and prepare new products, we need and want your input, both good and bad. Please contact us with your comments, concerns, and ideas for ways we can better serve you. Your feedback is welcomed, so we can work together to meet the security challenges facing the ICS community.

If you want to see an important or pertinent topic addressed in this forum, please send your suggestions to: ics-cert@hq.dhs.gov.

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL:

https://forms.us-cert.gov/ncsd-feedback/