

The PMC Group LLC

Engineering a better tomorrow today

Cybersecurity: Protecting Your Buildings - and Your Company

Michael Chipley, PhD GICSP PMP LEED AP
President

April 23, 2015

mchipley@pmcgroup.biz

Agenda

Cyber attacks on Building Control Systems and IT
New federal Acquisition and Procurement Language
Overview of Building Control Systems
Exploiting Building Control Systems
Protecting Building Control Systems

Operation Cleaver - Iran

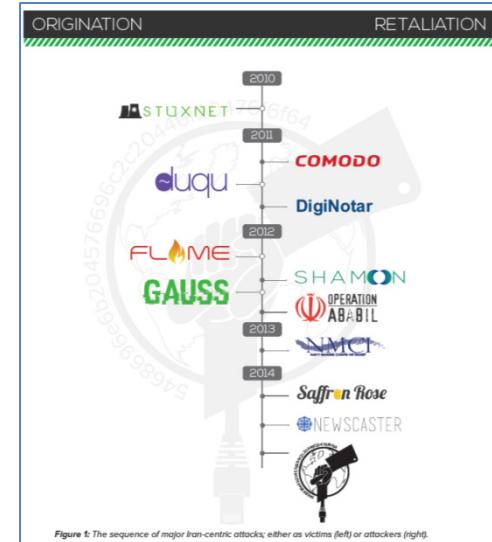


- Iranian team dubbed Tarh Andishan
- Believed to consist of at least 20 hackers and developers, collaborating on projects and missions to support Iranian interests
- Evolved skillset and uses a complex infrastructure to perform attacks of espionage, theft, and the ***potential destruction of control systems and networks***
- Over 50 victims, distributed around the globe
- 10 victims are headquartered in the US and include a major airline, a medical university, an energy company specializing in natural gas production, an automobile manufacturer, ***a large defense contractor, and a major military installation.***

WHY THE NAME CLEAVER?

The string cleaver is found several times in a variety of custom software used in Operation Cleaver, including inside the namespaces of their custom bot code TinyZBot, e:\projects\cleaver\trunk\zhoupin_cleaver\obj\x86\release\netscp.pdb

Targets and Access



- Targeting and compromise of transportation networks and systems
- Level of access seemed ubiquitous: Active Directory domains were fully compromised, along with entire Cisco Edge switches, routers, and internal networking infrastructure
- Fully compromised VPN credentials meant their ***entire remote access infrastructure and supply chain*** was under the control of the Cleaver team, allowing ***permanent persistence*** under compromised credentials
- Achieved ***complete access to airport gates and their security control systems***
- Gained access to PayPal and Go Daddy credentials allowing them to make fraudulent purchases and allowed ***unfettered access to the victim's domains***

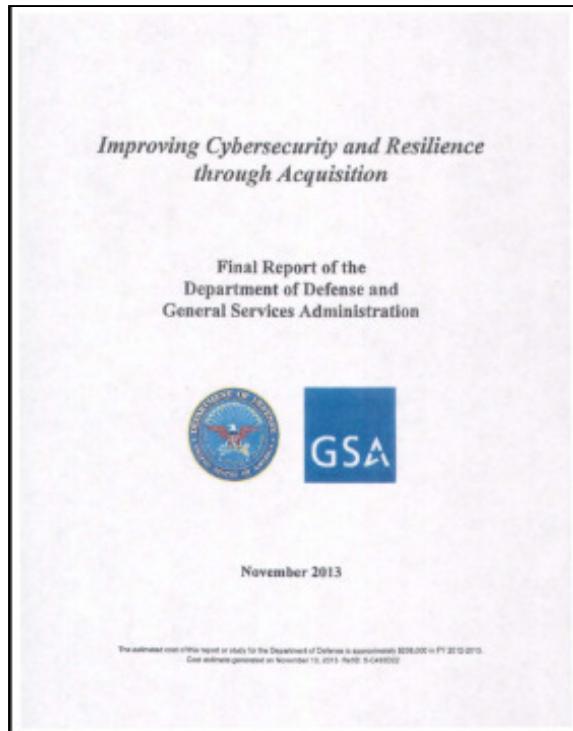
What's At Stake?

- Persian hacker names are used throughout the campaign including: Salman Ghazikhani, Bahman Mohebbi, Kaj, Parviz, Alireza, and numerous others.
- Numerous domains used in the campaign were registered in Iran
- Spearfishing using resumes, multiple domains were registered in order to make the download sites seem more realistic (Teledyne-Jobs.com, Doosan-Job.com, NorthropGrumman.net)
- ***To date it has successfully evaded detection by existing security technologies***
- ***Confirmed hacking into unclassified U.S. Navy computers in San Diego's NMCI (Navy Marine Corp Intranet)***
- Iran is no longer content to retaliate against the US and Israel alone, position themselves to impact critical infrastructure globally

Mitigation: identify their presence in your network, prevent them from expanding the scope of the compromise, and remove their access **immediately**.

GSA-DoD Acquisition Reform

Six reform recommendations:

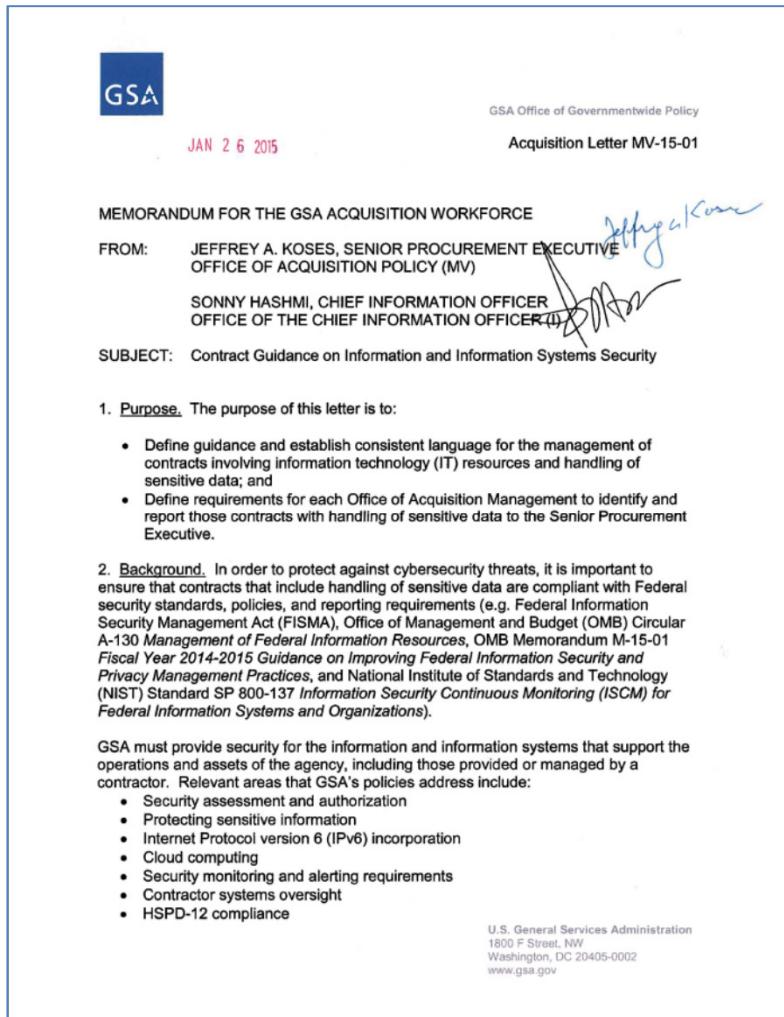


1. Institute baseline cybersecurity requirements as a condition of contract award for appropriate acquisitions
2. Include cybersecurity in acquisition training
3. Develop common cybersecurity definitions for federal acquisitions
4. Institute a federal acquisition cyber risk management strategy
5. Include a requirement to purchase from original equipment manufacturers, their authorized resellers, or other trusted sources
6. Increase government accountability for cyber risk management

<http://www.gsa.gov/portal/content/176547>

GSA IT Acquisition Memo Jan 2015

Appendix D



New Contract Language

The following language shall be included in the Statement of Work, or equivalent, for all procurements where contractors may require access to sensitive data, or use information technology (IT) resources.

[Begin Paragraph]

Safeguarding Sensitive Data and Information Technology Resources
In accordance with FAR 39.105, this section is included in the contract.

This section applies to all users of sensitive data and information technology (IT) resources, including awardees, contractors, subcontractors, lessors, suppliers and manufacturers.

Contract Cyber Risk Management Plan

- (e) Order Cybersecurity Risk Management Plan (OCRMP) Submittal, Review, and Acceptance
 - (1) Submittal.
 - (i) When submitting a proposal in response to any task order solicitation, Contractor shall **submit its approved CCRMP to the ordering contracting officer as an addendum to the proposal.**
 - (ii) If required by the task order solicitation, Contractor shall also provide an Order Cybersecurity Risk Management Plan (OCRMP) that includes additional information to address the specific security requirements of the task order solicitation.
- (f) Order Cybersecurity Risk Management Plan Update, Review, and Acceptance
 - (1) Updates.
 - (i) Contractor may update its OCRMP at any time after order award to ensure the Government is adequately assured of Contractor's continuous ability to provide appropriate cybersecurity in the deliverables it provides under the contract.

CCRMP based on NIST SP 800-53 R4

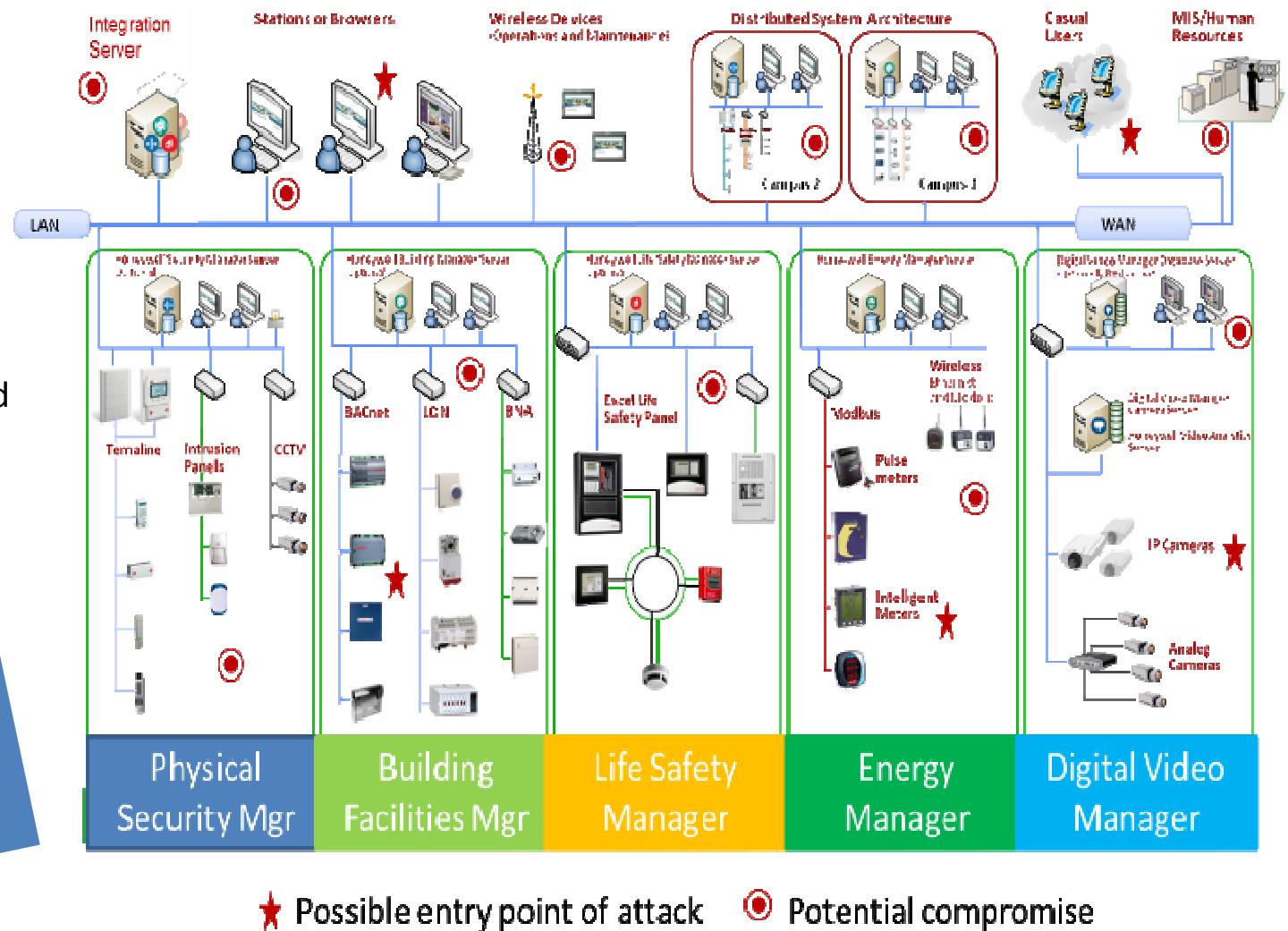
**Arlington Workshops: "How To" Workshop: Develop a Contract
Cybersecurity Risk Management Plan**

DoD Building ICS

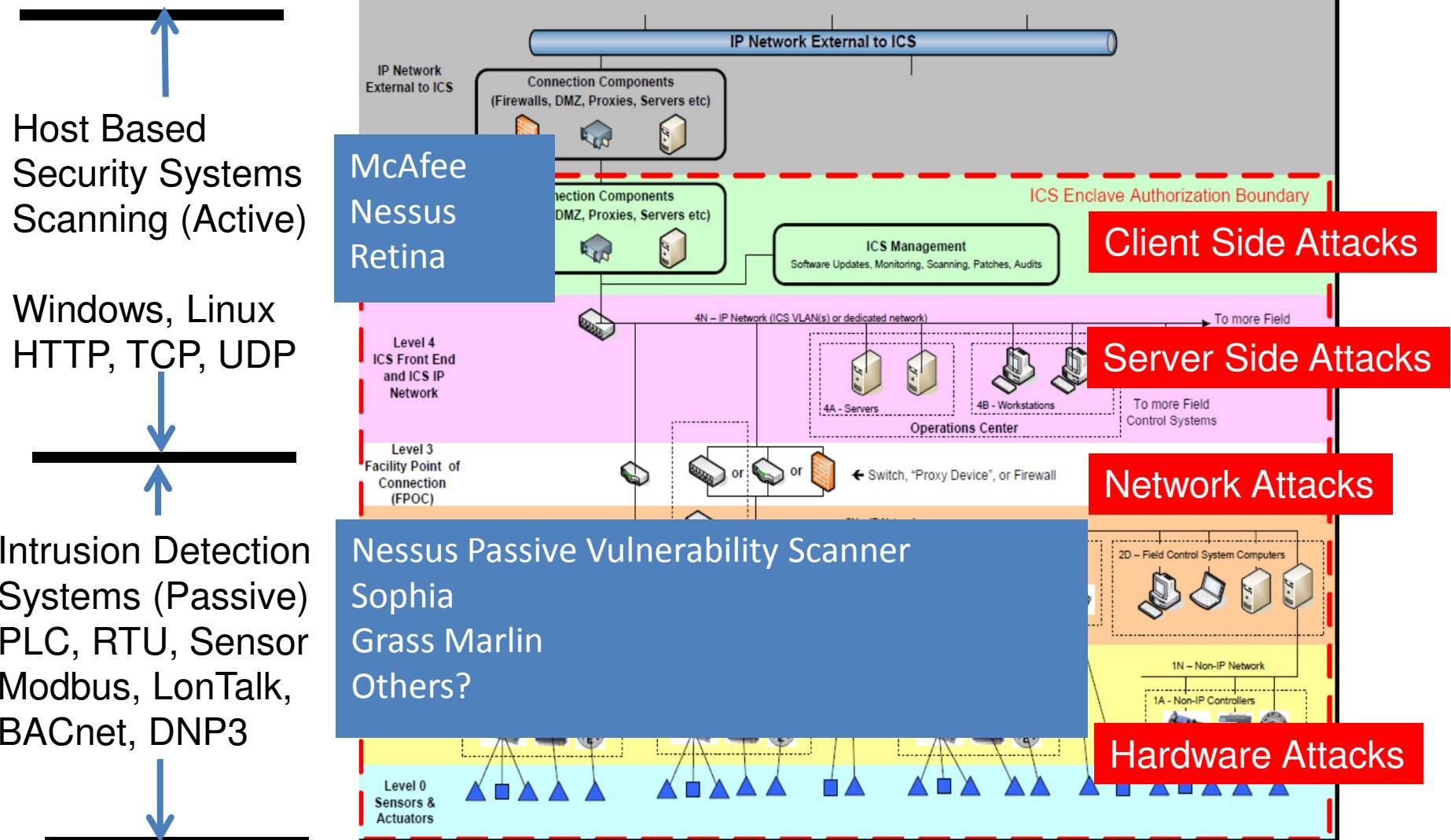
DoD Real Property Portfolio

- 48 countries
- 523 installations
- 4,855 Sites
- 562,600 buildings and structures
- 24.7 M acres
- \$847 B value

**What's in
Your
Building?**



Continuous Monitoring and Attack Surfaces



System & Terminal Unit Controllers, Actuators



JACE



Field Server



iLon Smart Server



VAV



L-switch



BAS Remote Server



Valve Actuator



Valve Actuator



Pressure Sensor



Temperature Sensor

Analog voltage, resistance, current signal is converted to digital and then IP

ICS Protocols

Internet Protocols

- IPv4 and IPv6
- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Hypertext Transfer Protocol (HTTP) - Port 80
- Hypertext Transfer Protocol Secure (HTTPS) - Port 443

Open Control Systems Protocols

- Modbus: Master/Slave - Port 502
- BACnet: Master/Slave - Port 47808
- LonWorks/LonTalk: Peer to Peer - Port 1679
- DNP3: Master/Slave - Port 20000
- IEEE 802.x - Peer to Peer
- Zigbee - Peer to Peer
- Bluetooth – Master/Slave

Proprietary Control Systems Protocols

- Tridium NiagraAX/Fox
- Johnson Metasys N2
- OSIsoft Pi System
- Many others...

Building Control System Protocols

Control systems are fundamentally different than IT

- Can be based on Master and Slaves or Peer to Peer
- Slaves have Registers and Coils
- Devices use several different programming languages to perform operations
- Not originally designed for security or encryption

Master = Client : sends requests for values in the address

Slave = Server : replies with data

Registers and Coils = memory locations

Typical file extensions:

*.ACD
*.CXP
*.ESD
*.ESX
*.LDA
*.LCD
*.LDO
*.LCX
*.plcproject
*.PRJ
*.PRT
*.RSP
*.QXD
*.SCD

Tools

Information Gathering

- **Google Search and Hacking**
- Google Earth
- The Harvester
- Recon-NG
- **Shodan**
- Costar

Network Discovery and Monitoring

- Nmap
- Snort
- Kismet
- Nessus
- McAfee
- **Sophia**
- Bandolier

Attack and Defend Tools

- Kali Linux (Backtrack)
- **SamuraiSTFU**
- **Wireshark**
- Gleg
- Windows PowerShell
- Windows Management Information Console
- Windows Enhanced Mitigation Tools
- Windows Sysinternals

Assessment Tools

- **DHS ICS-CERT Cyber Security Evaluation Tool (CSET)**

Virtual Machines

- VM Player
- Windows Hypervisor

Google Hacking

navy tridium bangor

Web Shopping News Maps Images More Search tools

About 403,000 results (0.43 seconds)

Search Results: Procurement Synopsis Database - NECO
<https://www.neco.navy.mil/synopsis/detail.aspx?id=367322> •
Aug 17, 2012 - Contact Points: Pam Pratt 360-396-0234 pamela.d.pratt@navy.mil ...
located in Naval Base Kitsap, Bremerton, WA, and Naval Base Kitsap, Bangor, WA.
... The NNRW ICS uses Tridium's Niagara AX based Architecture which ...

Z-Project Labor Agreement Inquiry, RM 1113414, Energy
www.govcb.com/Z-Project-Labor-Agreement-Inquiry-ADP135052223200...
Sep 30, 2000 - ... Bremerton, WA and Naval Base Kitsap at Bangor, Silverdale, WA.
... The NNRW ICS uses Tridium's Niagara AX based Architecture which ...

Naval Base Kitsap - Bangor - Military.com
www.military.com/base-guide/naval-base-kitsap--bangor • Military.com •
Naval Base Kitsap was created in 2004 by merging the former Naval Station
Bremerton with Naval Submarine Base Bangor. The Mission of Naval Base Kitsap
is ...
Missing: tridium

Daniel Ehrhart | LinkedIn
<https://www.linkedin.com/pub/daniel-ehrhart/8a/59/25b>
Richmond, Kentucky - Technical Training Specialist at GP Strategies Corporation
US Navy, May 2012 – Present (2 years 8 months) Bangor, WA. Coordinated ... 2013.
Awarded 3 Navy and Marine Core Achievement medals for performance while serving

<https://www.google.com/#q=navy+tridium+bangor>

Google Hacking

The screenshot shows a Microsoft Internet Explorer browser window with a red border. The address bar at the top contains the URL <https://www.neco.navy.mil/synopsis/detail.aspx?id=367322>. The title bar includes tabs for "Introduction to Cybersecuring ...", "Search Results: Procurement...", and the current page. The main content area displays a "SOURCES SOUGHT NOTICE" document. The document details a construction contract for repairing and modernizing industrial control systems (ICS) at Naval Base Kitsap, Bremerton, WA, and Naval Base Kitsap, Bangor, WA. It specifies the synopsis date as Aug 14, 2012, and the solicitation number as N4425513MKTG1. The document also includes contact information for Pam Pratt and a detailed description of the sources sought process.

SOURCES SOUGHT NOTICE

Subject: Z--Design / Build Construction Contract for repair and modernizing the Industrial Control System (ICS) located in Naval Base Kitsap, Bremerton, WA, and Naval Base Kitsap, Bangor, WA.

Synopsis Date: Aug 14, 2012

Contracting Office Address: N44255 NAVFAC NORTHWEST 1101 Tautog Circle Silverdale, WA

NAICS Code: 238210 Electrical Contractors and Other Wiring Installation Contractors

Classification Code: Z - Maintenance, Repair or Alteration of Real Property

Solicitation Number: N4425513MKTG1

Response Date: Aug 28, 2012

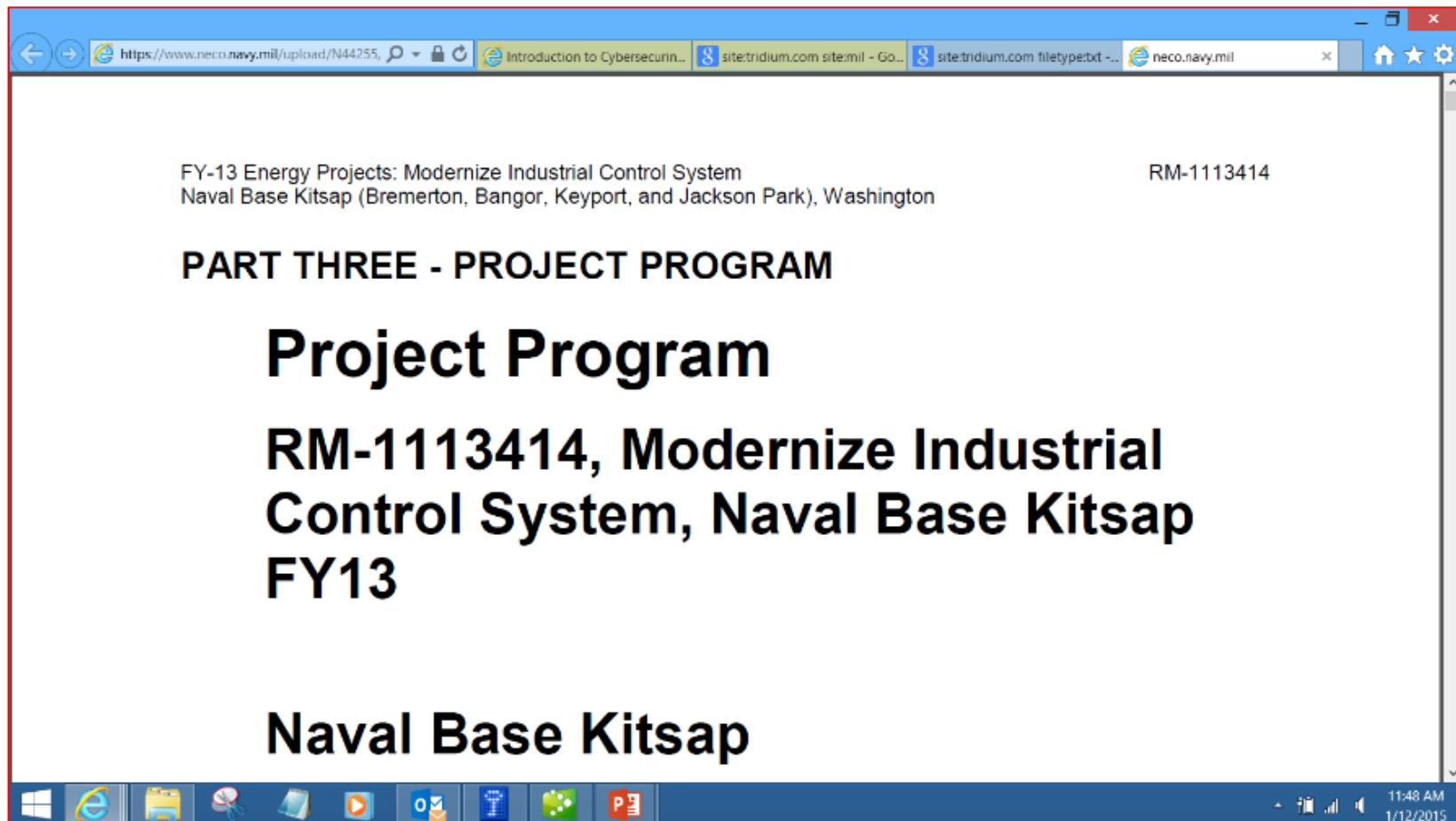
Archive Date: Sep 12, 2012

Contact Points: Pam Pratt 360-396-0234 pamela.d.pratt@navy.mil

Description: This is a Sources Sought Synopsis only. This is not a solicitation announcement and there are no Request for Proposal (RFP) documents to download. This synopsis is a market research tool being utilized to determine the availability of qualified Small Business sources prior to issuing an RFP. The Government is seeking qualified 8(a), HUBZONE, Service Disabled Veteran Owned Small Business (SDVOSB), and/or Small Business (SB) sources that are certified by the Small Business Administration (SBA) relative to NAICS classification 238210. The applicable size standard is \$14.0 M, average annual gross receipts for the preceding three fiscal years. Responses to this sources sought synopsis will be used to make appropriate acquisition decisions. After review of the responses to this sources sought synopsis, and if the Government plans to proceed with the acquisition, a solicitation announcement will be published in Federal Business Opportunities and NECO. Responses to this sources sought are not an adequate response to the solicitation announcement. No telephone calls will be accepted requesting a bid package or solicitation. There is no bid package or solicitation at this time. In order to protect the procurement integrity of any future procurement, if any, that may arise from this announcement, information regarding the technical point of contact will not be

<https://www.neco.navy.mil/synopsis/detail.aspx?id=367322>

Google Hacking



filetype:pdf -site:tridium.com site:mil

https://www.neco.navy.mil/upload/N44255/N4425513R40020005N4425513R40020005N44255-13-R-4002_Part_3_Draft.pdf

Shodan

The image shows a web browser window with two tabs open. The left tab is the Shodan homepage (<http://www.shodanhq.com/>). The header includes links for Main, Exploits, Research, Videos, Anniversary Promotion, Register, and Login. Below the header is a search bar with the word "SHODAN" and a search button. The main content features a large world map with red dots representing exposed devices. Text on the page includes "EXPOSE ONLINE DEVICES.", "WEBCAMS. ROUTERS.", "POWER PLANTS. IPHONES. WIND TURBINES.", "REFRIGERATORS. VOIP PHONES.", "TAKE A TOUR", and "FREE SIGN UP". Popular search queries listed are "default password". Below this is a "DEVELOPER API" section with a gear icon and a "LIVE" section with a lifebuoy icon. The right tab shows a search results page from Bing for "shodan hacking" (<http://www.bing.com/videos/search?q=shodan+hacking>). It displays a video player with a thumbnail showing a man speaking and several other video thumbnails below it. The video player has a caption that reads "this movie clip is a tiny pice of what you can do on this site. explore the site on your own." To the right of the video player is a sidebar with "Related Searches" including "YouTube Hacking Lazars", "YouTube Hacking", "Hacking Parody", "How To Hack YouTube", "YouTube Hackers", "How To Hack Everything", "YouTube Hacking", and "Hack A YouTube".

Shodan is to OT IP addresses as is Google is to text search

Tridium

The screenshot shows the Tridium website homepage. At the top, there's a navigation bar with links for North America, EMEA, Asia, and Latin America. Below the navigation is a large banner featuring two Boeing aircraft in a factory setting. The left side of the banner has text about Boeing and a "Click to read the Case Study" link. The right side of the banner has a "Case Study" link. Below the banner is a blue sidebar with various links: Corporate Info, Products & Services, Markets & Applications, Tridium News, Library, Partner Channels, Purchase, Tridium University, Tridium Asia Pacific, and Tridium EMEA. The main content area features a section titled "Solutions For Connecting Devices to the Enterprise". It includes a paragraph about Tridium's technology, a "Tech Guides available" section with links to "Using a VPN with Niagara Systems" and "Niagara[®] Hardening Guide", and the "NIAGARA SUMMIT 2014" logo. The bottom of the page shows a Windows taskbar with various icons and the date/time "10:39 AM 3/20/2014".

Boeing, the world's largest manufacturer of commercial jetliners maintains its reputation as an innovative leader by implementing Vyon Energy in their Renton, Washington production facilities.

Click to read the Case Study

1 2 3 4 5 6 7 8 9 10

Corporate Info
Products & Services
Markets & Applications
Tridium News
Library
Partner Channels
Purchase
Tridium University
Tridium Asia Pacific
Tridium EMEA

Boeing, the world's largest manufacturer of commercial jetliners maintains its reputation as an innovative leader by implementing Vyon Energy in their Renton, Washington production facilities.

Click to read the Case Study

1 2 3 4 5 6 7 8 9 10

Solutions For Connecting Devices to the Enterprise

Tridium is the global leader in open platforms, application software frameworks, automation infrastructure technology, energy management and device-to-enterprise integration solutions. Our technology and applications have fundamentally changed the way devices and systems connect, integrate and interoperate with each other and the enterprise.

Our configurable software frameworks extend connectivity, integration and interoperability to the millions of devices deployed in the market today and empowers manufacturers to develop intelligent equipment systems and smart devices that enable collaboration and communication between the enterprise and edge assets. Our platforms allow for building and managing complex monitoring, control, and

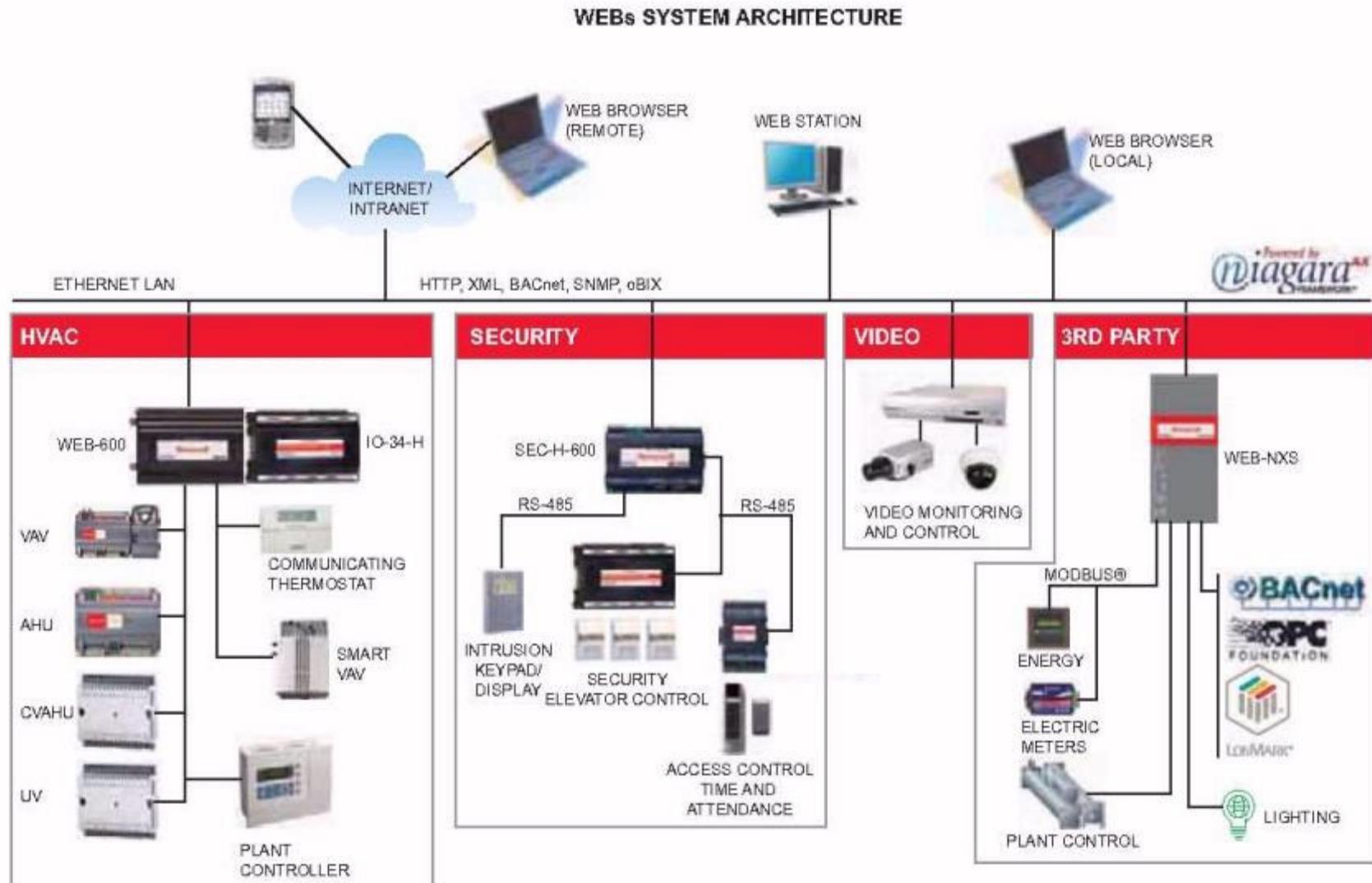
NIAGARA SUMMIT 2014

Tech Guides available

- Using a VPN with Niagara Systems
- Niagara[®] Hardening Guide

Links » 10:39 AM 3/20/2014

Tridium Architecture



Shodan – Tridium Search

The screenshot shows the Shodan search interface with the query 'tridium'. The results list several devices, each with a summary, location, and network details.

- 97.78.98.252**
Time Warner Cable
Added on 20.03.2014
Tampa, USA
rrcs-97-78-98-252.se.biz.rr.com
NetBIOS Response
Servername: TRIDIUM-PC
MAC: b8:ca:3a:84:86:4f
Names:
TRIDIUM-PC <0x0>
WORKGROUP <0x0>
TRIDIUM-PC <0x20>
WORKGROUP <0x1e>
WORKGROUP <0x1d>
_MSBROWSE__ <0x1>
- 116.6.58.158**
China Telecom Next Generation Carrier Network
Added on 20.03.2014
Guangzhou, China
NetBIOS Response
Servername: TRIDIUMPWS04
MAC: 00:50:b6:52:46:c3
Names:
TRIDIUMPWS04 <0x0>
TRIDIUM <0x0>
TRIDIUMPWS04 <0x20>
- 76.12.61.228**
HostMySite
Added on 18.03.2014
Newark, USA
Tridium station

The bottom navigation bar includes icons for Windows, Internet Explorer, File Explorer, Media Player, Task Manager, Task View, File History, and Print.

A login form titled 'VictorPark_Super' with fields for 'Username' and 'Password'. It features a key icon and a 'Login' button.

DDAN - Computer Search E... Login

VictorPark_Super

Username:

Password:

Login

Distech Controls

The screenshot shows the homepage of the Distech Controls website (<http://www.distech-controls.com/>). The header features a large image of three professionals in a modern office setting. To the left, there's a sidebar with categories: OFFICES & COMMERCIAL BUILDINGS, EDUCATION, HOSPITALS & HEALTHCARE, and MORE. The main navigation bar includes links for HOME, SOLUTIONS, PRODUCTS, RESOURCES, ABOUT US, NEWS AND EVENTS, CONTACT US, and YOUR LOCATION. The PRODUCTS menu is currently open, showing sub-options like Overview, Building Management System, Energy Management, HVAC Control, Integrated Room Control Solution, Open-to-Wireless™, Lighting Control, Access Control and CCTV, Room Devices, Peripherals, Product Certifications, and Products Tutorials. A sidebar on the right lists Resources & Popular Links, including Authorized Partner Client Log-in, Visit the Consulting Engineer Resource Center, Contact Us for More Information, Building Automation Products for HVAC, Lighting and Access Control, and Energy Management Solutions for. The bottom of the page shows a taskbar with various icons and system status information.

Shodan – Distech Search



HTTP/1.0 401 Unauthorized

WWW-Authenticate: Digest realm="**Niagara-Admin**", qop="auth", algorithm="**MD5**",
nonce="UvdraWNmNDAwNjE1ODc4NzBhYTc5NjMyYzlkYTk3NTg1ZDQy"

Content-Length: 56

Content-Type: text/html

Niagara-Platform: QNX

Niagara-Started: 2013-8-3-4-11-32

Baja-Station-Brand: **distech**

Niagara-HostId: Qnx-NPM2-0000-12EA-FDCC

Server: **Niagara Web Server/3.0**

Google Hacking-Database



<http://www.exploit-db.com/google-dorks/>

Google Hacking DB Search

The screenshot shows a Windows desktop environment with a web browser displaying the Exploit Database website at <http://www.exploit-db.com/search/?action=search>. The browser's address bar also shows the URL <http://www.exploit-db.com/search/?action=search>.

The Exploit Database homepage features a large logo "EXPLOIT DATABASE" with a bug icon. To the right, there are links for "blog", "exploit", and "F". It also displays statistics: "Currently Archiving 31708 Exploits" and "Updated (CVE And Archive): Wed Jan 7 2015".

The main content area includes a navigation menu with buttons for HOME, GHDB, ABOUT, REMOTE, LOCAL, WEB, DOS, SHELLCODE, PAPERS, SEARCH, and SUBMIT.

Below the menu, there are three promotional boxes:

- Intrusion Detection Tool**
at gfi.com/ids-software
Detect Intruders & Security Gaps w/ GFI EventsManager! Free Trial
- Server Scan: Free**
at qualys.com/Server-Scan
Accurate, Fast Detection of Server Vulnerabilities. Get Free Scan!
- Enterprise File Sharing**
at egnyte.com/Business-File-Sharing
Securely Access Files & Collaborate Anywhere, Any Device. Free Trial!

A large "Search" section is present, showing search results for "Honeywell". The results table has columns for Date, D, A, V, Description, Plat., and Author.

Date	D	A	V	Description	Plat.	Author
2013-03-13	green checkmark	-	green checkmark	Honeywell HSC Remote Deployer ActiveX Remote Code Execution	windows	metasploit
2013-01-10	red downward arrow	-	green checkmark	Honeywell Tema Remote Installer ActiveX Remote Code Execution	windows	metasploit

The taskbar at the bottom shows various pinned icons, and the system tray indicates the date as 1/7/2015 and the time as 4:55 PM.

Google Hacking Diggity Project

The screenshot shows a web browser window with the URL <http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/#searchdiggity>. The page is titled "Google Hacking Diggity Project". On the left, there's a sidebar with sections for "ATTACK TOOLS", "SEARCHDIGGITY", "HACKING DICTIONARIES", and "HACKING GOOGLE CUSTOM SEARCH". The main content area features a large heading "Attack Tools" and a descriptive paragraph about search tools. Below that is a section for "SEARCHDIGGITY" with a sub-section for "SearchDiggity v 3". A screenshot of the SearchDiggity software interface is shown, displaying a search bar with the word "SEARCHDIGGITY". The status bar at the bottom right of the screenshot shows the date and time: "11:31 AM 1/12/2015".

<http://www.bishopfox.com/resources/tools/google-hacking-diggity/attack-tools/#searchdiggity>

Google Hacking Diggity Project

The screenshot shows the Google Hacking Diggity software interface. At the top, there is a navigation bar with tabs: Google, CodeSearch, Bing, LinkFromDomain, DLP, Flash, Malware, PortScan, NotInMyBackyard, BingMalware, and Shodan. The Shodan tab is highlighted with a red box and has a red arrow pointing to it from the text "Enter SHODAN API key". Below the navigation bar is a toolbar with Simple and Advanced buttons, a SCAN button, a Settings button, and a Cancel button. A large red box highlights the "API Key:" input field, which contains the placeholder "Create". To the right of the input field is a "Hide" checkbox. A red callout bubble points to the "API Key:" field with the text "Enter SHODAN API key". On the left side, there is a "Query Appender" section with an orange border and a "Queries" section with a tree view of search categories. The main area displays a table of search results for SCADA systems. The table has columns: Category, Search String, URL, Hostnames, City, and Country. The results are as follows:

Category	Search String	URL	Hostnames	City	Country
SCADA	Niagara Web Server	http://193.185.169.90/			Finland
SCADA	Niagara Web Server	http://12.171.57.87/			United States
SCADA	Niagara Web Server	http://70.168.40.243/	wsip-70-168-40-243.	Cleveland	United States
SCADA	Niagara Web Server	http://216.241.207.94/	sciop-ip94.scinternet.	Colorado City	United States
SCADA	Niagara Web Server	http://206.82.16.227/	niagarafred.norleb.k1	Lancaster	United States
SCADA	Niagara Web Server	http://184.187.11.158/		Omaha	United States

Below the table, there are two tabs: Output and Selected Result. The Selected Result tab is active and shows the following HTTP response headers:

```
HTTP/1.0 302 Moved Temporarily
location: http://70.168.40.243/login
content-type: text/html; charset=UTF-8
content-length: 116
set-cookie: niagara_audit=guest; path=/
server: Niagara Web Server/3.5.34
```

A red callout bubble points to the "Selected Result" tab with the text "Finding SCADA systems via SHODAN Diggity".

Kali Linux

The screenshot shows a web browser window with the URL <http://www.kali.org/> in the address bar. The page content is the Kali Linux homepage. At the top, there is a navigation bar with links for BLOG, DOWNLOADS, TRAINING, DOCUMENTATION, COMMUNITY, and ABOUT US. Below the navigation bar, there is a large banner featuring the Kali Linux logo and the tagline "PENETRATION TESTING, REDEFINED." with the subtitle "the quieter you become, the more you are able to hear". To the left of the banner, there is a text box containing promotional text about Kali Linux and its history. The bottom of the screen shows a Windows taskbar with various icons and the system tray.

The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - [What's new ?](#)

KALI LINUX
"the quieter you become, the more you are able to hear"

**PENETRATION TESTING,
REDEFINED.**

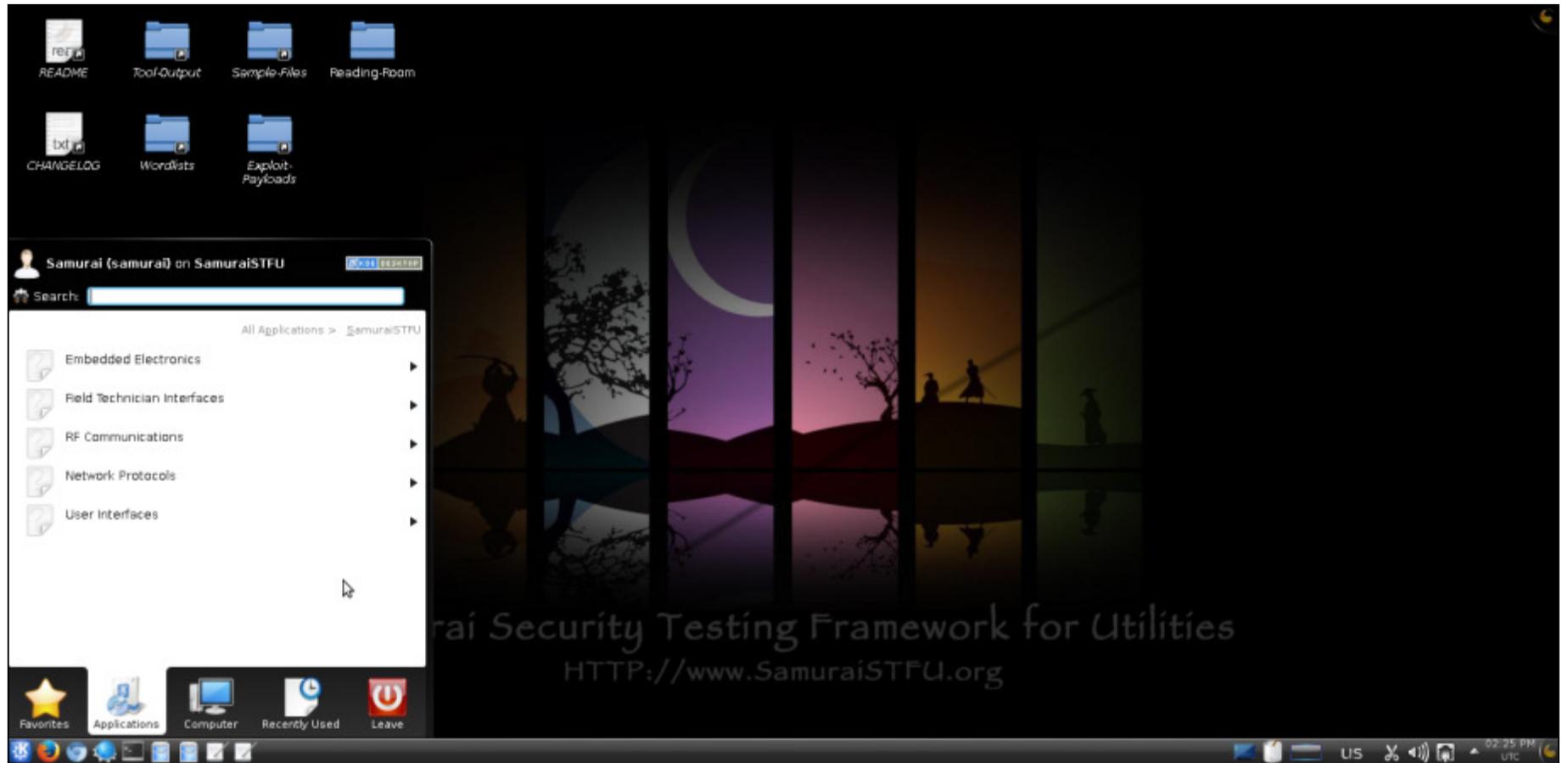
A Project By Offensive Security

External Penetration Test

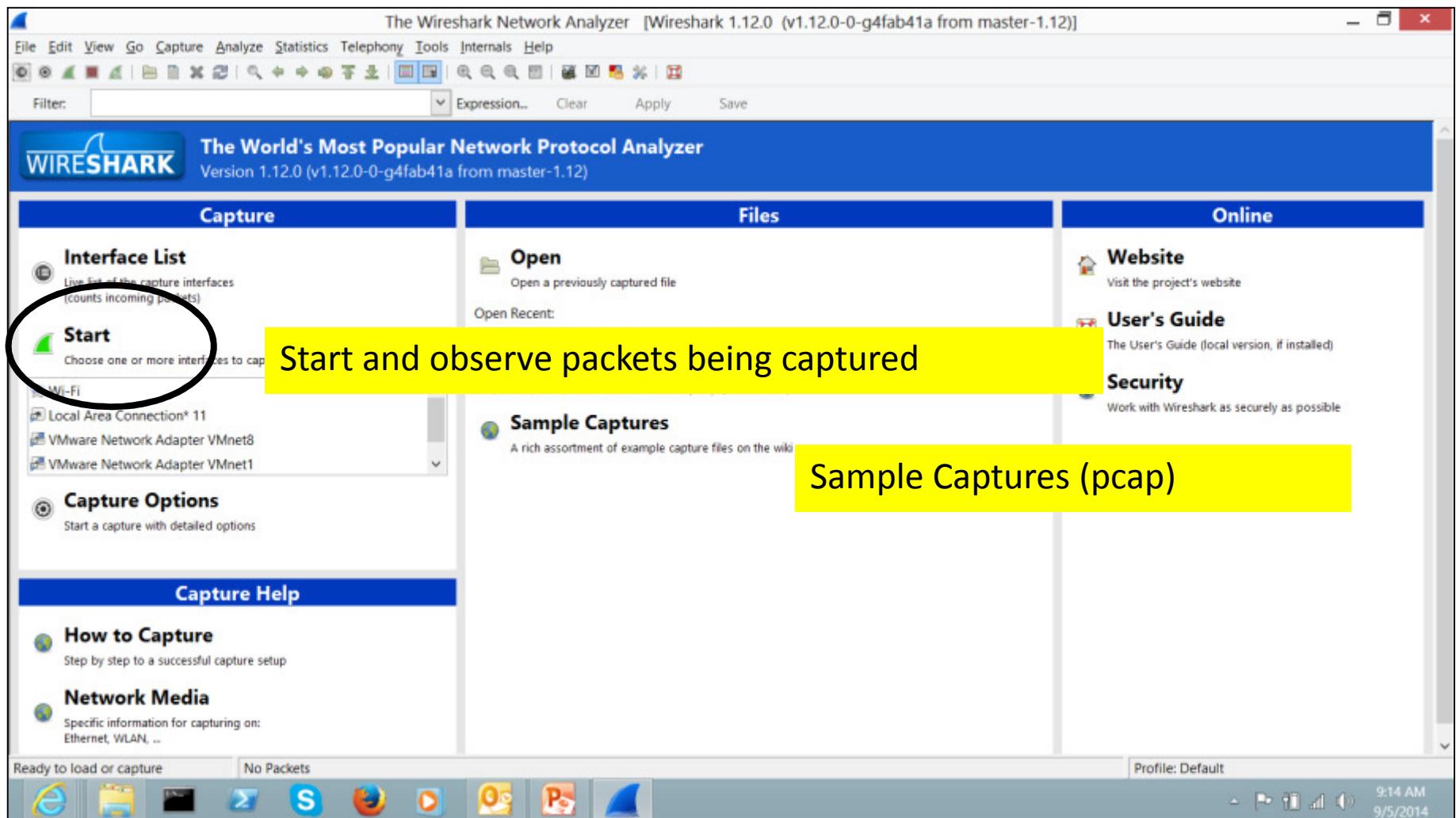
Links 4:42 PM
3/27/2014

<http://www.kali.org/>

SamuraiSTFU Applications



Wireshark Home



<https://www.wireshark.org/about.html>

Wireshark Active Packet Capture

Capturing from Wi-Fi [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
73	56.516391074:56:12:5b:6a:9e	Broadcast		ARP	60	Who has 192.168.1.1? Tell 192.168.1.101
74	56.5219900ArrisGro_59:41:8a	Broadcast		ARP	60	Who has 192.168.1.1? Tell 192.168.1.100
75	64.6187010169.254.1.239		169.254.1.255	UDP	78	Source port: 7500 Destination port: 7500
76	65.7982680169.254.1.239		255.255.255.255	UDP	1179	Source port: 21302 Destination port: 21302
77	69.8366830169.254.1.239		169.254.1.255	UDP	60	Source port: 51096 Destination port: 5000
78	71.1376530fe80::847:942:9a74:ff02::1:2			DHCPv6	145	Solicit XID: 0x463783 CID: 00010001b23fc2dc0ea12adc0f
79	72.3775460192.168.1.4		255.255.255.255	UDP	124	Source port: 49519 Destination port: 1211
80	72.5706630192.168.1.1		224.0.0.1	IGMPv3	50	Membership Query, general
81	74.6673620169.254.1.239		169.254.1.255	UDP	78	Source port: 7500 Destination port: 7500

Frame 1: 42 bytes on wire (336 bits)
Interface id: 0 (\Device\NPF_{...})
Encapsulation type: Ethernet (1)
Arrival Time: Sep 8, 2014 11:36:42.627520000 Eastern Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1410190602.627520000 seconds
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 42 bytes (336 bits)
Capture Length: 42 bytes (336 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:arp]
[Coloring Rule Name: ARP]
[Coloring Rule String: arp]
Ethernet II, Src: 00:7f:28:0d:0e:4f (00:7f:28:0d:0e:4f), Dst: 94:39:e5:75:e1:9f (94:39:e5:75:e1:9f)
Destination: 94:39:e5:75:e1:9f (94:39:e5:75:e1:9f)
Source: 00:7f:28:0d:0e:4f (00:7f:28:0d:0e:4f)
0000 94 39 e5 75 e1 9f 00 7f 28 0d 0e 4f 08 06 00 01 .9.u.... (.0....
0010 08 00 06 04 00 01 00 7f 28 0d 0e 4f c0 a8 01 01 (.0....
0020 00 00 00 00 00 00 c0 a8 01 05

Frame (frame), 42 bytes Packets: 81 · Displayed: 81 (100.0%) Profile: Default

Windows Taskbar icons: Internet Explorer, File Explorer, Task View, Start, Search, Firefox, YouTube, File Manager, Power Options, Network, Wi-Fi, Battery, Volume, Date/Time (11:37 AM, 9/8/2014)

Wireshark BACnet pcap

Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12) bacnet-stack-services.cap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Char Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.13	192.168.0.255	BACnet-	53	Simple-ACK acknowledgeAlarm[2]
2	22.717118	192.168.0.13	192.168.0.255	BACnet-	64	Unconfirmed-REQ who-Has
3	22.745865	00:60:2d:00:15:d5	Broadcast	BACnet-	60	Unconfirmed-REQ who-Has
4	22.765855	192.168.0.5	192.168.0.13	BACnet-	74	Unconfirmed-REQ device,61 device,61
5	200.636101	192.168.0.13	192.168.0.255	BACnet-	69	Unconfirmed-REQ device,61 device,61
6	200.664755	00:60:2d:00:15:d5	Broadcast	BACnet-	60	Unconfirmed-REQ device,61 device,61
7	200.684766	192.168.0.5	192.168.0.13	BACnet-	74	Unconfirmed-REQ device,61 device,61
8	279.455576	192.168.0.13	192.168.0.255	BACnet-	64	Unconfirmed-REQ timeSynchronization
9	279.485292	00:60:2d:00:15:d5	Broadcast	BACnet-	60	Unconfirmed-REQ timeSynchronization

Frame 1: 53 bytes on wire (424 bits), 53 bytes captured (424 bits)

Ethernet II, Src: 00:0c:6e:b0:3c:15 (00:0c:6e:b0:3c:15), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Internet Protocol Version 4, Src: 192.168.0.13 (192.168.0.13), Dst: 192.168.0.255 (192.168.0.255)

User Datagram Protocol, Src Port: 47808 (47808), Dst Port: 47808 (47808)

Source Port: 47808 (47808)
Destination Port: 47808 (47808)
Length: 19
Checksum: 0x01b [validation disabled]
[Stream index: 0]

BACnet Virtual Link Control
Type: BACnet/IP (Annex J) (0x81)
Function: Original-Unicast-NPDU (0x0a)
BVLC-Length: 4 of 11 bytes BACnet packet length

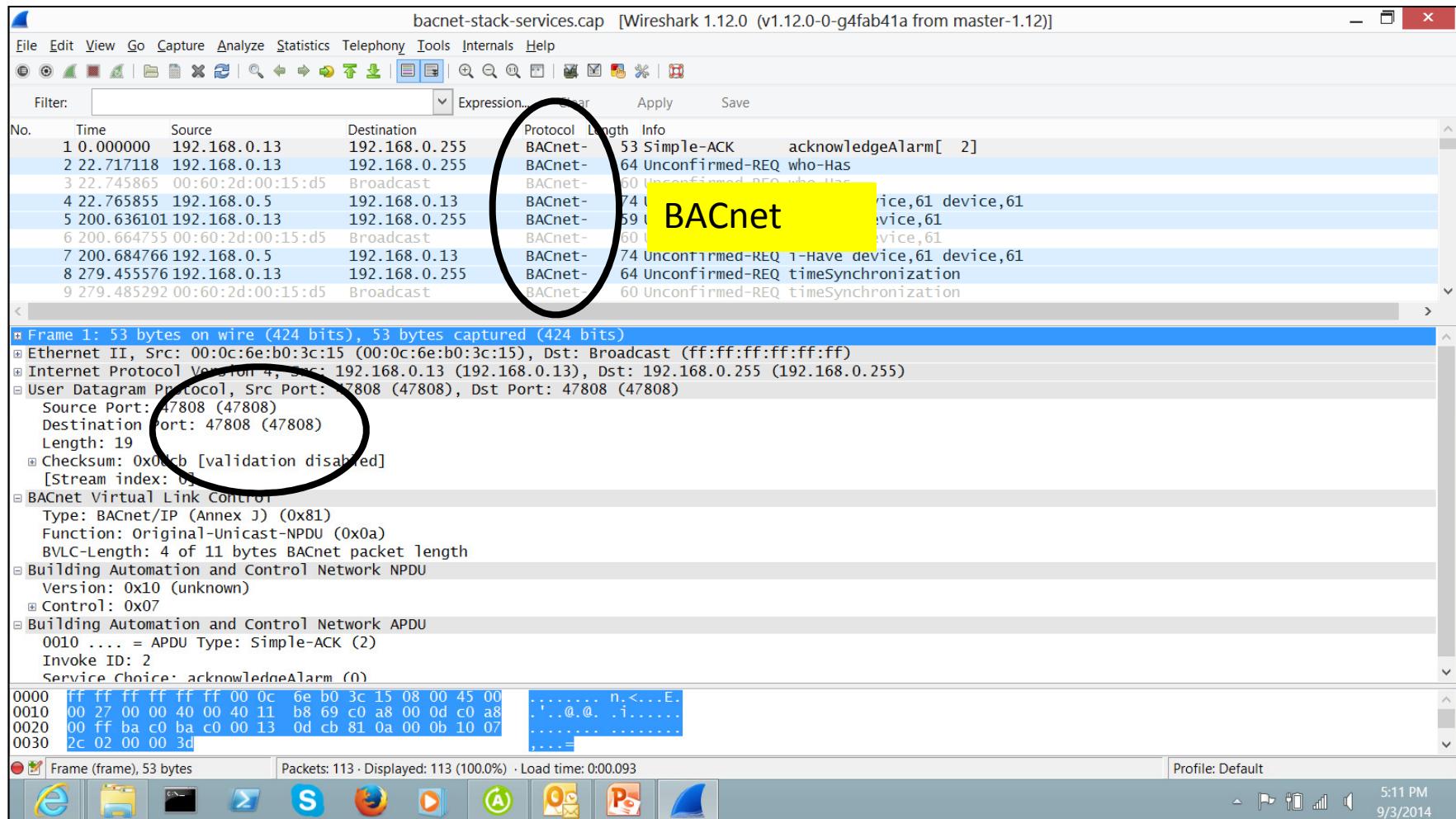
Building Automation and Control Network NPDU
Version: 0x10 (unknown)
Control: 0x07

Building Automation and Control Network APDU
0010 = APDU Type: Simple-ACK (2)
Invoke ID: 2
Service Choice: acknowledgeAlarm (0)

0000 ff ff ff ff ff 00 0c 6e b0 3c 15 08 00 45 00 :..... n.<...E.
0010 00 27 00 00 40 40 11 b8 69 c0 a8 00 0d c0 a8 :....@. .i....
0020 00 ff ba c0 ba c0 00 13 0d cb 81 0a 00 0b 10 07 :.....
0030 2c 02 00 00 3d :....=

Frame (frame), 53 bytes Packets: 113 · Displayed: 113 (100.0%) · Load time: 0:00.093 Profile: Default

5:11 PM 9/3/2014



NIST SP 800-82 R2

NIST National Institute of Standards and Technology
Information Technology Laboratory

SEARCH CSRC: GO

CONTACT SITE MAP

Computer Security Division CSD

Computer Security Resource Center CSRC

CSRC Home About CSD Projects / Research Publications News & Events

Hot Topics

- + [Cybersecurity Framework](#)
- + [Cryptographic Standards Development Process Review](#)
- + [Attribute Based Access Control \(ABAC\)](#)
- + [FIPS 140-2 Crypto Module Validation List](#)

Useful Resources

- + [2013 CSD Annual Report](#)
- + [A-Z List of Projects](#)
- + [Cryptographic Toolkit](#)
- + [FISMA Implementation Project](#)
- + [National Vulnerability Database \(NVD\)](#)

 [Sign Up for Email Alerts from NIST's Computer Security](#)

Computer Security Resource Center (CSRC)

The Computer Security Division's (CSD) Computer Security Resource Center (CSRC) facilitates broad sharing of information security tools and practices, provides a resource for information security standards and guidelines, and identifies key security web resources to support users in industry, government, and academia.

CSRC is the primary gateway for gaining access to [NIST computer security publications](#), standards, and guidelines plus other useful security-related information.

News

February 9, 2015
NIST announces the [final public draft release of Special Publication 800-82, Revision 2, Guide to Industrial Control System \(ICS\) Security](#)

January 29, 2015
[Errata Update for Special Publication 800-53, Revision 4](#)

January 26, 2015

CSD Security Events

[Workshop on Upcoming Special Publications Supporting FIPS 201-2](#)
March 3-4, 2015
NIST, Gaithersburg, MD

[2015 FISSEA Conference](#)
March 24-25, 2015
NIST, Gaithersburg, MD

[Workshop on Cybersecurity in a Post-Quantum World](#)
April 2-3, 2015
NIST Gaithersburg, MD

[+ MORE EVENTS](#)



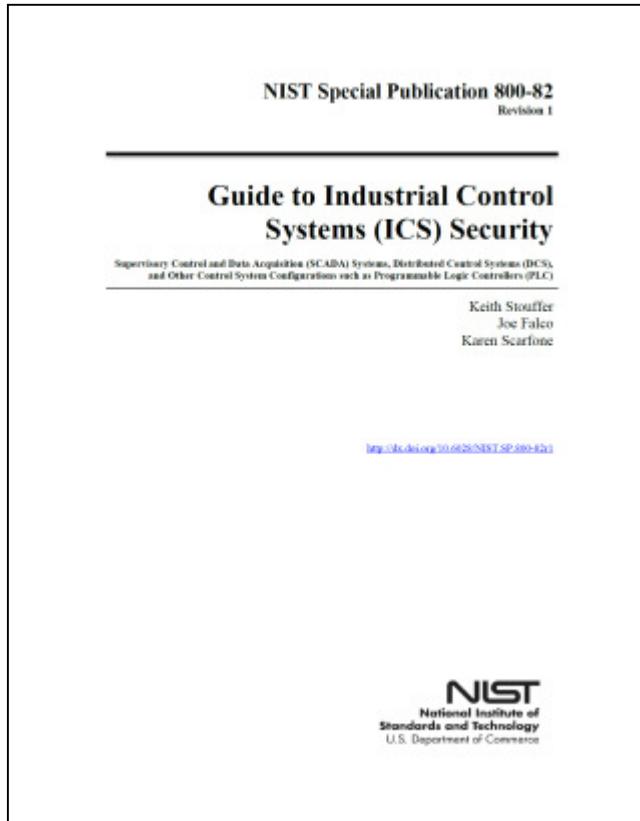
ITL Bulletin

February 2015
NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization

Draft Publications Request

Section 2.5 added per DoD request to address ‘other-than-industrial’ control systems

Standards – NIST SP 800-82 R2



This document provides guidance for establishing secure industrial control systems (ICS). These ICS, which include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) are often found in the industrial control sectors.

This document provides an overview of these ICS and typical system topologies, identifies typical threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks.

- 800-82 Rev 1 was released May 2013 - has 800-53 Rev 3 Appendix I and 600+ controls
- 800-82 Rev 2 is scheduled for Final release spring 2015 – has 800-53 Rev 4 800+ controls, **Appendix G ICS Overlay**

NIST SP 800-82 R2 Key Security Controls

Inventory

- CM-8 Information System Component Inventory
- PM-5 Information System Inventory
- PL-7 Security Concept of Operations
- PL-8 Information Security Architecture
- SC-41 Port and I/O Device Access
- PM-5 Information System Inventory

Central Monitoring

- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- IR-5 Incident Monitoring
- IR-6 Incident Reporting
- PE-6 Monitoring Physical Access
- PM-14 Testing, Training and Monitoring
- RA-5 Vulnerability Scanning
- SC-7 Boundary Protection
- SI-4 Information System Monitoring
- SI-5 Security Alerts, Advisories, and Directives

Test and Development Environment

- CA-8 Penetration Testing
- CM-4 Security Impact Analysis
- CP-3 Contingency Training
- CP-4 Contingency Plan Testing and Exercises
- PM-14 Testing, Training and Monitoring

Critical Infrastructure

- CP-2 Contingency Plan
- CP-6 Alternate Storage Site
- CP-7 Alternate Processing Site
- CP-10 Information System Recovery and Reconstitution
- PE-3 Physical Access Control
- PE-10 Emergency Shutoff
- PE-11 Emergency Power
- PE-12 Emergency Lighting
- PE-13 Fire Protection
- PE-14 Temperature and Humidity Controls
- PE-17 Alternate Work Site
- PM-8 Critical Infrastructure Plan

Acquisition and Contracts

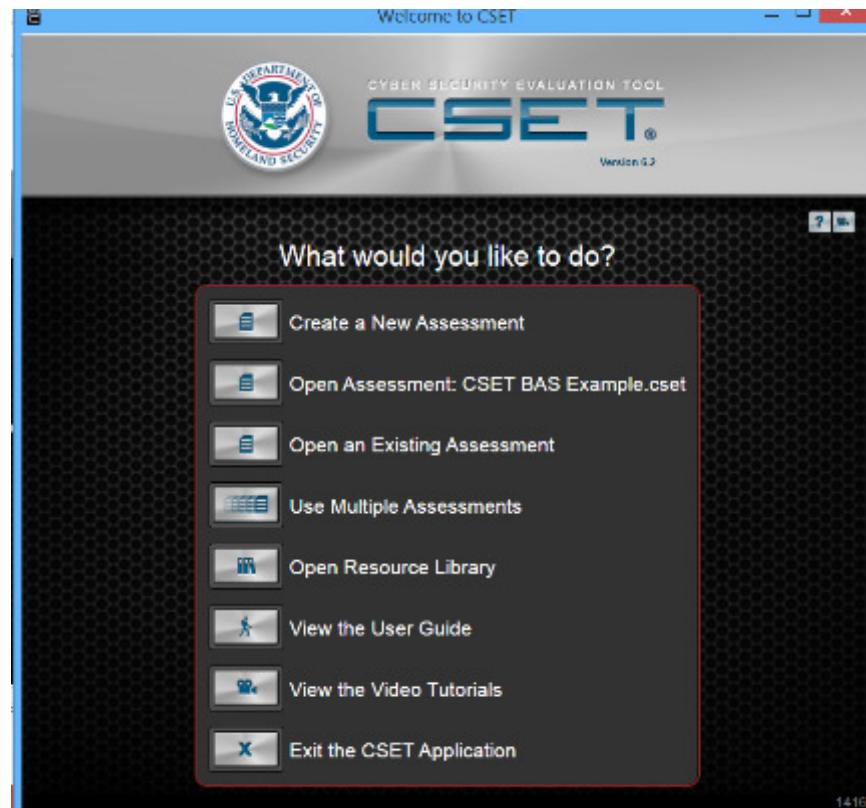
- AU-6 Audit Review, Analysis, and Reporting
- CA -7 Continuous Monitoring
- SA-4 Acquisitions
- PM-3 Information System Resources
- PM-14 Testing, Training and Monitoring

Inbound Protection,
Outbound Detection

DHS CSET



- Stand-alone Software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

www.ics-cert.us-cert.gov/Downloading-and-Installing-CSET

DHS NCCIC and ICS-CERT CSET

National Cybersecurity and Communications Integration Center

<http://www.us-cert.gov/nccic/>

DHS CSET 6.2 Tool

- NIST Cybersecurity Framework
- NIST 800-30
- NIST 800-53 Rev 3
- NIST 800-53 Rev 4
- NIST 800-82 Rev 1
- NIST 800-82 Rev 2
- NIST 1108
- NISTR 7628
- NERC CIP



The screenshots illustrate the integration between the National Cybersecurity and Communications Integration Center (NCCIC) and the DHS CSET 6.2 Tool. The top image shows the official website of the US-CERT, which includes a prominent NCCIC logo. The middle image shows a specific page within the CSET framework related to the Control Systems Security Program (CSSP). The bottom image shows the main user interface of the CSET application, providing a central hub for various cybersecurity functions.

New Assessment Form

Cyber Security Self Evaluation Tool (CSET)

File Windows Help
CSET INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY DOCUMENT LIBRARY

ASSESSMENT:

Assessment Name: Untitled Assessment 1 Facility Name: Assessment Date: 3/27/2014 15

City or Site Name: State, Province, or Region:

PRINCIPAL ASSESSOR:

Name: Email: Telephone:

DESCRIPTION OF ASSESSMENT: **COMMENTS:**

ADDITIONAL CONTACTS:

EXECUTIVE SUMMARY:

Cyber terrorism is a real and growing threat. Standards and guides have been developed, vetted, and widely accepted to assist with protection from cyber attacks. The Cyber Security Evaluation Tool (CSET) includes a selectable array of these standards for a tailored assessment of cyber vulnerabilities. Once the standards were selected and the resulting question sets answered, the CSET created a compliance summary, compiled variance statistics, ranked top areas of concern, and generated security recommendations.

Links 1:16 PM 3/27/2014



Standards Home - Step 1 Assessment Mode

The screenshot shows the CSET software interface. At the top, there's a menu bar with 'File', 'Windows', and 'Help'. Below it is a toolbar with icons for 'INFORMATION', 'STANDARDS', 'DIAGRAM', 'QUESTIONS', 'ANALYSIS', and 'REPORTS'. A 'RESOURCE LIBRARY' button is also present. The main area has a 'QUICK START' button followed by the text 'Start with a basic assessment OR follow the steps below...'. A large red header bar says 'STEP 1 - Assessment Mode'. Below it, a text box says: 'Most users should select the "Questions Based" option for a comprehensive evaluation based on questions rather than requirements.' Another text box says: 'To see the exact requirements for a specific standard, choose the "Standard Requirements Based" option. This would be common for regulated sectors where the precise wording is important.' A third text box says: 'Choose the "Cybersecurity Framework Based" option to perform a risk-based cybersecurity evaluation using the Framework for Improving Critical Infrastructure Cybersecurity.' Underneath these, there's a question: 'What approach would you like to take to perform a Cybersecurity evaluation?' with three radio button options: 'Questions Based' (selected), 'Standard Requirements Based', and 'Cybersecurity Framework Based'. Below this are two more red header bars: 'STEP 2 - Questions and Standards' and 'STEP 3 - Security Assurance Level (SAL)'. At the bottom, there are navigation buttons for 'INFORMATION', 'PREVIOUS', 'NEXT', and 'DIAGRAM'. The taskbar at the very bottom shows various system icons and the date/time '1:15 PM 9/24/2014'.

Step 2 - Questions and Standards

Cyber Security Self Evaluation Tool (CSET) - Untitled Assessment 1.cset

File Windows Help CSET INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY DOCUMENT LIBRARY

QUICK START Start with a basic assessment OR follow the steps below...

STEP 1 - Assessment Mode ►

STEP 2 - Questions and Standards ▾

General Control System Standards:

- Universal Questions
- Key Questions
- NIST Special Publication 800-82
- NIST Special Publication 800-82 Rev 1
- NIST Special Publication 800-53 Rev 3 App I
- NIST Special Publication 800-82 Rev 2

Information Technology (IT) Specific Standards:

- NIST Special Publication 800-53 Rev 3
- NIST Special Publication 800-53 Rev 4
- NIST Special Publication 800-53 Rev 4 App J

Requirements Mode Only Standards:

- Catalog of Recommendations Rev 7
- Consensus Audit Guidelines (CAG)
- DOD Instruction 8500.2

Sector Specific Standards:

- CFATS Risk-Based Performance Standards Guide 8-Cyber
- INGAA Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry
- NEI DB-09 Cyber Security Plan for Nuclear Power Reactors
- NERC CIP-002 through CIP-009 Rev 3
- NERC CIP-002 through CIP-009 Rev 4
- NISTIR 7628 Guidelines for Smart Grid Cyber Security, Vol. 1
- NRC Regulatory Guide 5.71
- TSA Pipeline Security Guidelines April 2011

Committee on National Security Systems Instruction (CNSSI) 1253:

- CNSSI No. 1253 Baseline
- CNSSI No. 1253 Industrial Control System (ICS) Overlay
- CNSSI No. 1253 (ICS) Overlay Version 1

1:20 PM
9/24/2014

Step 3 Questions

NIST Security Access Level (SAL) Determination

NIST Level:	High		
SAL VALUES			
Adjusted for System Questions	CONFIDENTIALITY HIGH	INTEGRITY HIGH	AVAILABILITY HIGH
Based on Information Type	HIGH	HIGH	HIGH

STEP 1 - NIST Guide ► ?

STEP 2 - Information Types ► ?

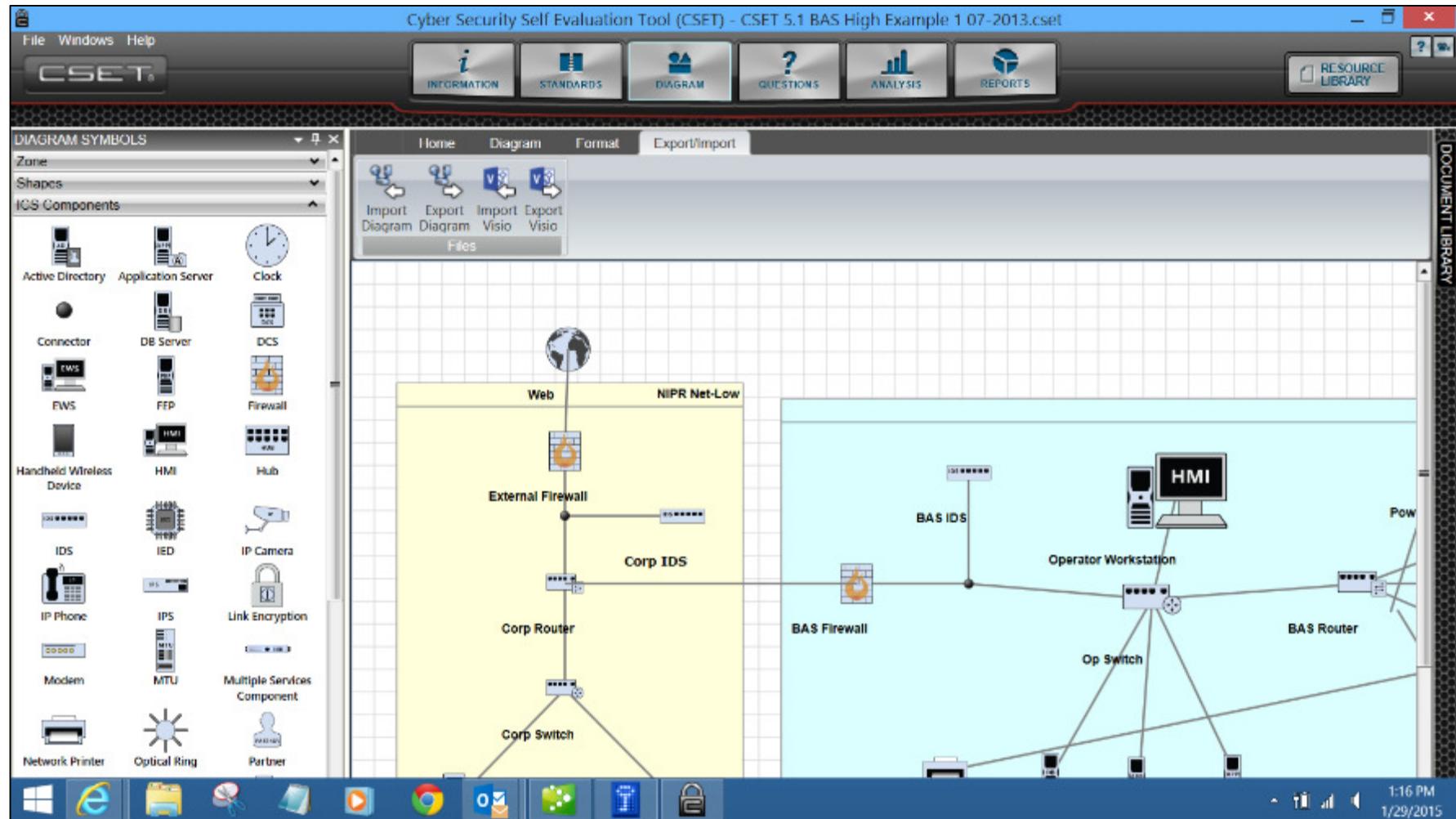
STEP 3 - Questions ▼ ?

#	Question	Yes	No
1	Does aggregation of information on this system reveal sensitive patterns and plans, or facilitate access to sensitive or critical systems?	<input checked="" type="radio"/>	<input type="radio"/>
2	Does/could access to this system result in some form of access to other more sensitive or critical systems (e.g., over a network)?	<input checked="" type="radio"/>	<input type="radio"/>
3	Are there extenuating circumstances such as: The system provides critical process flow or security capability, the public visibility of the system, the sheer number of other systems reliant on its operation, or the overall cost of the systems replacement?	<input checked="" type="radio"/>	<input type="radio"/>
4	Would unauthorized modification or destruction of information affecting external communications (e.g., web pages, electronic mail) adversely affect operations or seriously damage mission function and/or public confidence?	<input type="radio"/>	<input checked="" type="radio"/>
5	Would either physical or logical destruction of the system result in very large expenditures to restore the system and/or require a long period of time for recovery?	<input checked="" type="radio"/>	<input type="radio"/>
6	Does the mission served by the system, or the information that the system processes, affect the security of critical infrastructures and key resources?	<input checked="" type="radio"/>	<input type="radio"/>
7	Does the system store, communicate, or process any privacy act information?	<input type="radio"/>	<input checked="" type="radio"/>
8	Does the system store, communicate, or process any trade secrets information?	<input type="radio"/>	<input checked="" type="radio"/>

Links »

9:58 AM
7/17/2013

Diagram – Tools, Templates, Inventory



Questions – Family, Detail, Info

Cyber Security Self Evaluation Tool (CSET) - CSET 5.1 BAS High Example 2.07-2013.cset

File Windows Help

CSET INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY

All > SP800-53 R4 > Access Control

Access Control Met Unmet N/A ALT

QUESTION CATEGORIES DOCUMENT LIBRARY

1. The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number].

2. The organization:

- Develops, documents, and disseminates to [Assignment: organization-defined personnel or roles]:
 - An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
 - Procedures to facilitate the implementation of the access control policy and associated access controls; and
- Reviews and updates the current:
 - Access control policy [Assignment: organization-defined frequency]; and
 - Access control procedures [Assignment: organization-defined frequency]

3. The organization:

- Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
- Assigns account managers for information system accounts;
- Establishes conditions for group and role membership;
- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- Monitors the use of, information system accounts;
- Notifies account managers:
 - When accounts are no longer required;
 - When users are terminated or transferred; and
 - When individual information system usage or need-to-know changes;
- Authorizes access to the information system based on:
 - A valid access authorization;
 - Intended system usage; and
 - Other attributes as required by the organization or associated missions/business functions;
- Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and
- Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

4. The organization employs automated mechanisms to support the management of information system accounts.

The information system automatically [Selection: removes, disables] temporary and emergency accounts after [Assignment: organization-defined time period for each type of account].

The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [Assignment: organization-defined personnel or roles]

5. The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to log out].

(a) Monitors information system accounts for [Assignment: organization-defined atypical use]; and

Windows Internet Explorer File Search Control Panel Mail Microsoft Word Microsoft Excel Microsoft PowerPoint Microsoft OneNote Microsoft Word Microsoft Word 10:44 AM 2/22/2015

Analysis - Dashboard

Cyber Security Self Evaluation Tool (CSET)

File Windows Help CSET INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY

Assessment Compliance

Overall Standards Components

0 25 50 75 100 110

Components Summary Results

Yes No NA
 Alternate Unanswered

Standards Answers Summary

Yes No NA
 Alternate Unanswered

Top Categories of Concern

Access Control Account Management Audit and Accountability Continuity Configuration Management Communication Protection

0 10 20 30 40 50 60 70

Security Assurance Level:

Very High Confidentiality
High Integrity
Moderate Availability
Low
None

Summary of Results by Selected Standards

SP800-82 Requirements CNSSI 1253 Requirements 800-53 R3 Requirements

0 20 40 60 80 100

Percentage

Yes No N/A
 Alt Unanswered

Network Warnings **Top Concerns** **Unanswered Questions** **Questions With Comments** **Questions Marked for Review**

QUESTIONS PREVIOUS NEXT REPORTS

Links 12:08 PM 7/17/2013

Reports

Cyber Security Self Evaluation Tool (CSET)

File Windows Help

CSET.

INFORMATION STANDARDS DIAGRAM QUESTIONS ANALYSIS REPORTS RESOURCE LIBRARY

Report Builder

Select the report(s) you want to create and the file type then click the 'Create' button to create reports for your assessment. The 'Detail Options' button will allow you to determine what sections to include in the Detail Report before you create it.

EXECUTIVE SUMMARY SITE SUMMARY DETAIL OPTIONS SECURITY PLAN CREATE

PDF DOC DOCX

Select All Select All

Detail Report Options **Detail Report Standards Options**

Assessment Information Network Components

Executive Summary Standards Compliance

Document Library Component Diagram

Evaluation Of Selected Standards Network Component Analysis

Component Compliance Findings & Recommendations

Security Assurance Level Ranked Subject Areas

Summary of Ranked Questions Questions Marked For Review

Questions with Alternate Justification

DOCUMENT LIBRARY



Links 2:03 PM 3/27/2014

System Security Plan

SITE CYBER SECURITY PLAN
CONTROL SYSTEMS CYBER SECURITY EVALUATION



CYBER SECURITY EVALUATION TOOL
CSET

Untitled Assessment 1
3/27/2014
Assessor:

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland Security

CYBER SECURITY EVALUATION

3. Risk Analysis

A good security plan will require that a risk evaluation is performed to determine the level of necessary rigor and cost benefit analysis for the level of controls selected. If not yet performed yet it is recommended that the general risk analysis be performed. A good risk assessment should include an evaluation of the value of the protected assets and information, an examination of the consequences to the organization in the event of a successful attack, an examination of the threat if possible, and the cost of implementing mitigating controls.

$\text{threats} \times \text{vulnerability} \times \text{asset value} = \text{total risk}$

$\text{total risk} - \text{countermeasures} = \text{residual risk}$

Consequence

The examination of the consequences of an attack should include if control systems were maliciously accessed and manipulated to cause harm in a worst case scenario.

- How many people could sustain injuries requiring a hospital stay?
- How many people could be killed?
- Estimate the potential cost of losing capital assets or the overall economic impact. (Consider the cost of site buildings, facilities, equipment, etc.)
- Estimate the potential cost in terms of economic impact to both the site and surrounding communities. (Consider any losses to community structures and use and any costs associated with displacement.)
- Estimate the potential cost of environmental cleanup to the site and surrounding communities. (Consider the cost for cleanup, fines, mitigation, long term monitoring, etc.)

Threat

The threat portion of the equation can be deduced from the recommended implementation priorities list. The priorities are set based on incident data collected at the ICS-CERT watch floor and subject matter experts as of the time of publication of CSET. Top priorities are controls that mitigate the most actively exploited vulnerabilities with the most significant consequences.

Cost Benefit Analysis

The cost of implementing controls with respect to the additional security provided is the final step in selecting the controls to implement.

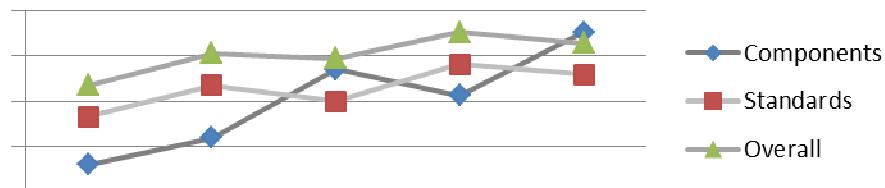
3.1. Basic Model

Traditional security models define three areas of consideration Confidentiality, Integrity, and Availability. The security plan should address each of these areas with respect to data and systems.

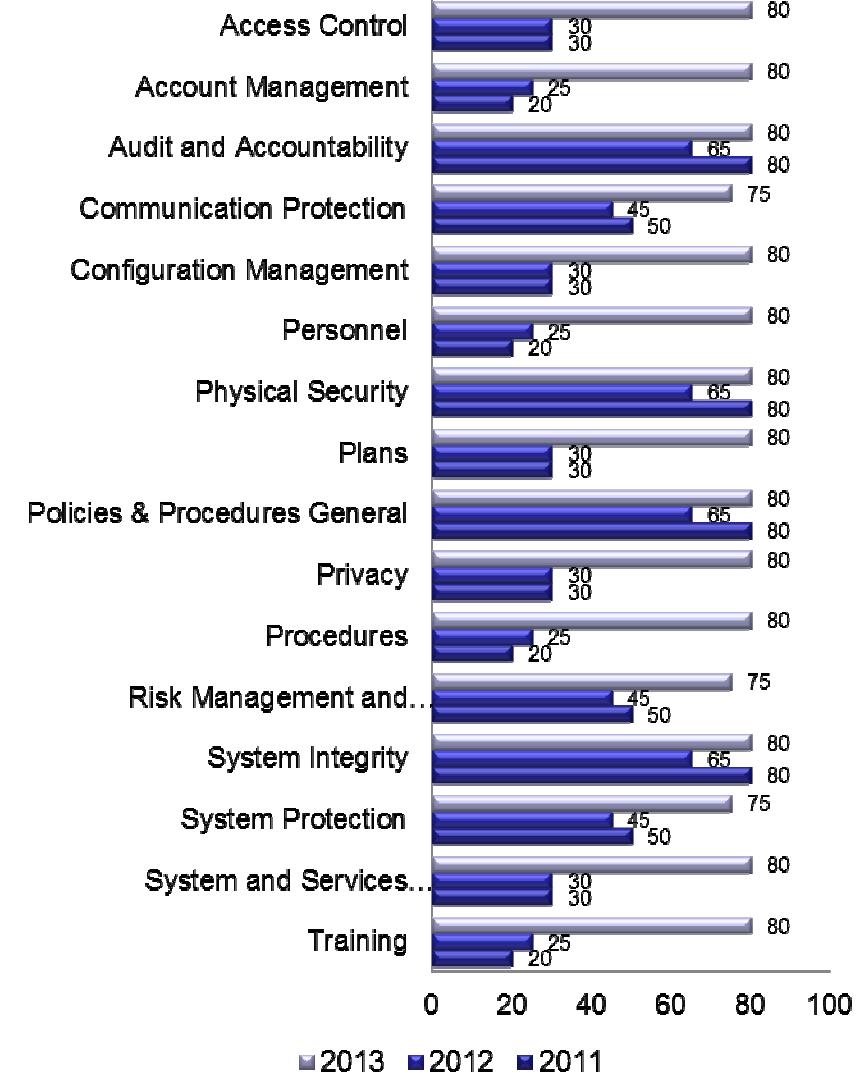
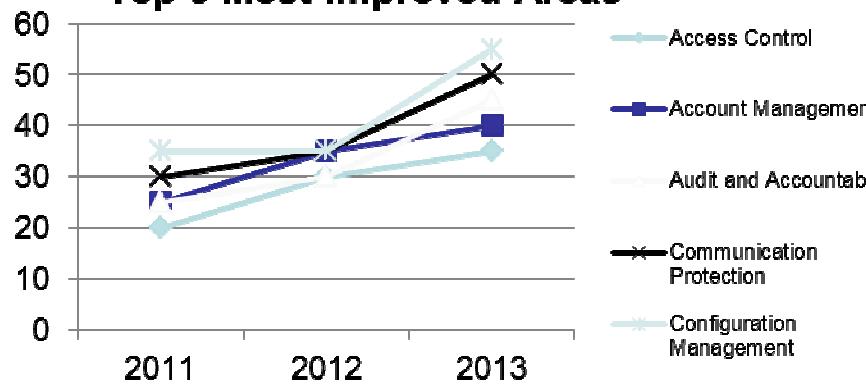
CSET Untitled Assessment 1 Page 14

Trending

Overall Trends

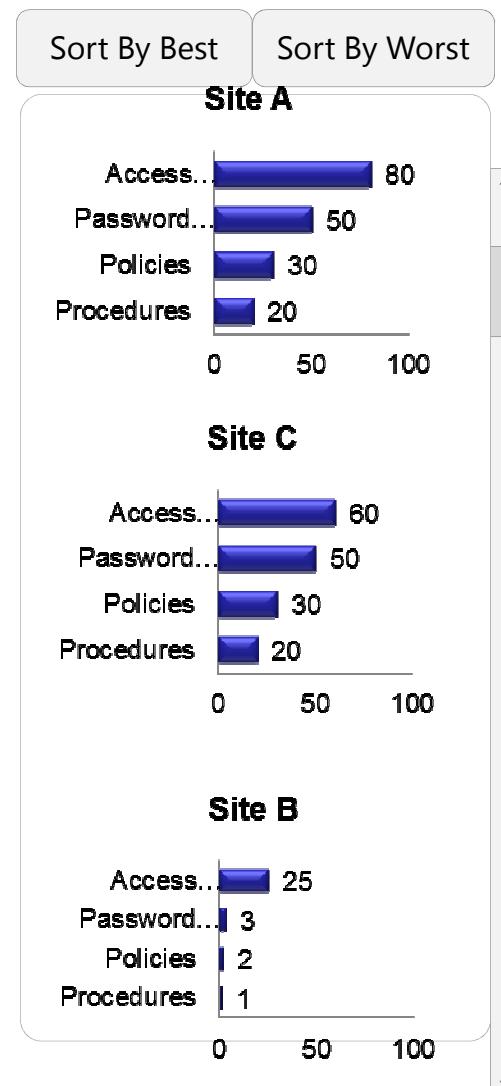
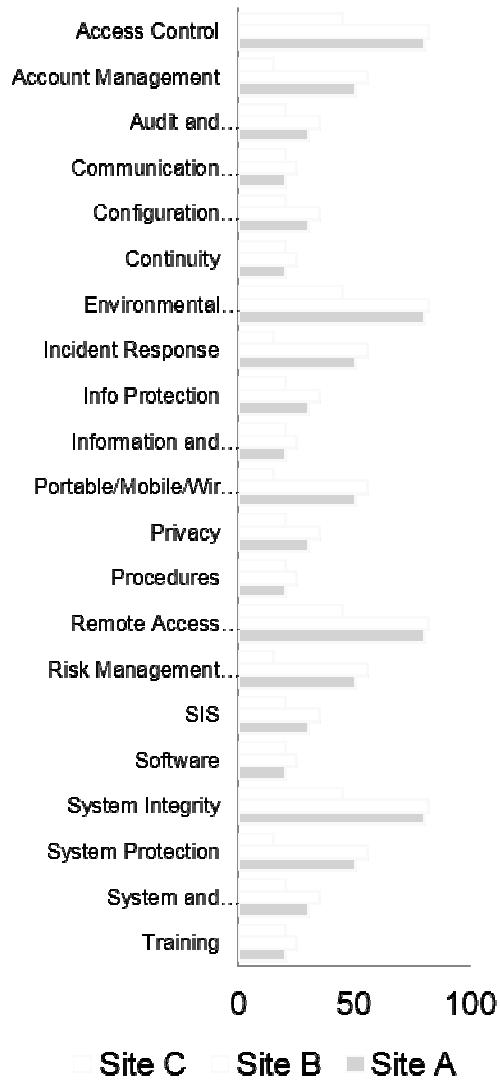
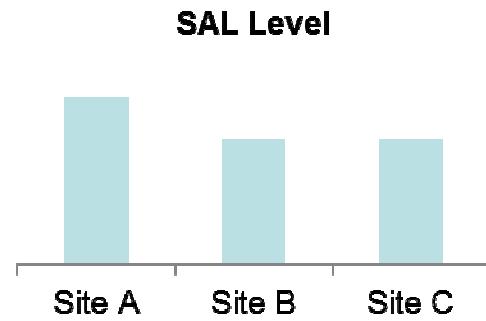
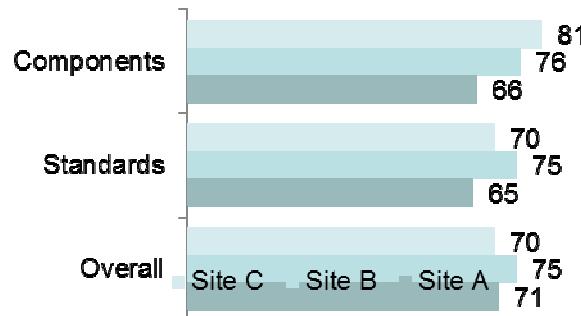


Top 5 Most Improved Areas



Compare

Site	Total Questions Answered	Yes	No
Site A	560	300	260
Site B	342	300	42
Site C	268	152	116



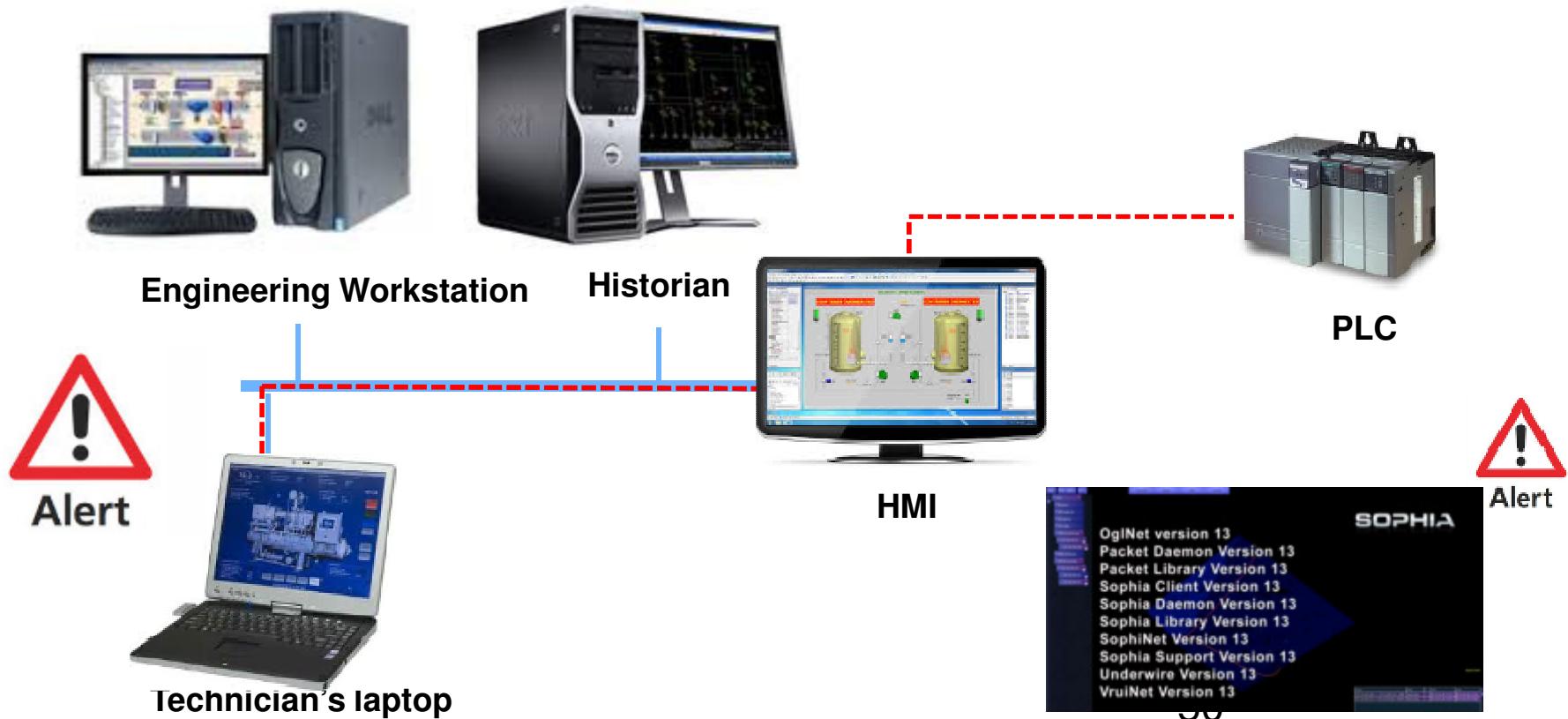
SOPHIA

The screenshot shows a Microsoft Internet Explorer browser window displaying the NexDefense website. The page features a dark header with the company logo and navigation links for Products, About Us, Careers, and Contact. Below the header is a video player showing a binary code sequence (1010101010101010) with a play button in the center. To the right of the video, a section titled "Empowering Control System Professionals" discusses the company's software for Industrial Control Systems (ICS). Further down the page, three main sections are visible: "Video: Fictional Cyber Attack", "What is Sophia?", and "Sophia Beta II Sign-Up Is Open". Each section includes descriptive text and a blue call-to-action button. At the bottom of the page is a footer with links for Company, LinkedIn, Twitter, and U.S. Federal Contractor, along with a toolbar and system status indicators.

http://nexdefense.com/?ao=1

SOPHIA

- Sophia can baseline approved/expected communication behavior
- Alert on communication sessions that are suspect/unexpected
- Example: DB Technician laptop should never send a Modbus command to the PLC



WBDG Cybersecurity Resource Page



The screenshot shows a web browser displaying the WBDG Cybersecurity Resource Page. The page has a header with the WBDG logo and navigation links for Home, About, Contact, Site Map, Log In, and Search. Below the header is a main content area with a sidebar on the left containing a list of design guidance topics. The main content area features a section titled "Cybersecurity" by Michael Chipley PhD, PMP, LEED AP, The PMC Group LLC, last updated 10-15-2013. The content discusses Industrial Control Systems (ICS) and their integration with IT systems, mentioning Stuxnet, Duqu, Flame, and Shamsheen malware. A sidebar on the right provides related resource pages and a view resource page index.

WBDG a program of the National Institute of Building Sciences

DESIGN GUIDANCE PROJECT MANAGEMENT OPERATIONS & MAINTENANCE DOCUMENTS & REFERENCES TOOLS CONTINUING EDUCATION BIM

A-C D-H I-R S-W

[Home](#) > Cybersecurity

Cybersecurity

By Michael Chipley PhD, PMP, LEED AP, The PMC Group LLC
Last updated: 10-15-2013

INTRODUCTION

Industrial Control Systems (ICS) are physical equipment oriented technologies and systems that deal with the actual running of plants and equipment, include devices that ensure physical system integrity and meet technical constraints, and are event-driven and frequently real-time software applications or devices with embedded software. These types of specialized systems are pervasive throughout the infrastructure and are required to meet numerous and often conflicting safety, performance, security, reliability, and operational requirements. ICSs range from building environmental controls (HVAC, [lighting](#)), to systems such as the electrical power grid. With the increasing interconnectivity of ICS to the internet, the ICS can be an entry point into the organization's other IT systems.

Within the controls systems industry, ICS systems are often referred to as Operational Technology (OT) systems. Historically, the majority of OT systems were proprietary, analog, vendor supported, and were not internet protocol (IP) enabled. Systems key components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), Physical Access Control Systems (PACs), Intrusion Detection Systems (IDSs), closed circuit television (CCTV), fire alarm systems, and utility meters have become digital and IP enabled. OT systems use Human Machine Interfaces (HMIs) to monitor the processes, versus Graphical User Interfaces for IT systems. Most current ICS systems and subsystems are now a combination of Operational Technologies (OT) and Information Technologies (IT).

The Stuxnet, Duqu, Flame and Shamsheen malware were specifically designed to target ICS and cause physical damage to the processes or equipment. Stuxnet "spoofed" the integrity of the uranium centrifuges and caused the centrifuges to overspin and self-destruct, while the operators console showed the system was operating within normal parameters. The Duqu malware looks for information that could be useful in attacking industrial control systems. Its purpose is not to be destructive; the known components are trying to gather information. The Flame malware looks for engineering drawings, specifications, and other technical details about the systems and records audio, screenshots, keyboard activity, and network traffic. The program also records Skype conversations and can turn infected computers into Bluetooth beacons which attempt to download contact information from nearby Bluetooth-enabled devices. The most recent malware attack, Shamsheen, destroyed over 30,000 Saudi Aramco work stations. Shamsheen is capable of spreading to other

COMMENT ON THIS PAGE
BOOKMARK AND SHARE

RELATED RESOURCE PAGES

- Construction Operations Building Information Exchange (COBIE)
- Electric Lighting Controls
- High-Performance HVAC
- Smart Controls

VIEW RESOURCE PAGE INDEX

THIS PAGE CONTAINS LINKS TO

CONSTRUCTION
EIA
ASE

Icons at the bottom include: Home, Project Management, Operations & Maintenance, Documents & References, Tools, Continuing Education, BIM, and Search.

<http://www.wbdg.org/resources/cybersecurity.php>

Cybersecuring Buildings Workshops

The screenshot shows the homepage of the National Institute of Building Sciences (NIBS). The header features the NIBS logo and the tagline "An Authoritative Source of Innovative Solutions for the Built Environment". A navigation menu at the top includes links for About, Councils & Projects, Membership, Resources, News, Events, and Contact. The main content area displays a news article titled "Institute Workshops to Focus on Cybersecurity of Building Control Systems" dated Friday, March 28, 2014. The article discusses the increasing reliance on building control systems and the need for cybersecurity. To the right, there is a sidebar for "Community Search" with a search bar and a "LATEST NEWS" section listing recent articles. At the bottom, there is a footer with social media icons for YouTube, Facebook, Google+, and LinkedIn.

News & Press: News Releases

[Email to a Friend](#)

Institute Workshops to Focus on Cybersecurity of Building Control Systems

Friday, March 28, 2014

[Share |](#)

New Dates Added

The nation's buildings are increasingly relying on building control systems (otherwise known as operational technology) that are Internet-enabled. These systems provide critical services that allow a building to meet the functional and operational needs of building occupants, but they can also be easy targets for hackers and people with malicious intent. Attackers can exploit these systems to gain unauthorized access to facilities; cause physical destruction of building equipment; be used as an entry point to infect or sabotage traditional information technology (IT) systems and data; and expose an organization to significant financial obligations to contain and eradicate malware or recover from a cyber event.

Two new workshops sponsored by the National Institute of Building Sciences will help architects, engineers, contractors, owners, facility managers, maintenance engineers, physical security specialists, information assurance professionals and essentially anyone involved with implementing cybersecurity in the facility life cycle to learn best practice techniques to better protect their facilities.

The Introduction to Cybersecuring Building Control Systems Workshop and the Advanced Cybersecuring Building Control Systems Workshop are both built around Executive Order 13636—Improving Critical Infrastructure Cybersecurity, issued on February 19, 2013; the National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework, issued on February 12, 2014; the draft NIST Special Publication (SP) 800-82 Rev. 2 Industrial Control Systems Security Guide, to be issued in April 2014; and the draft U.S. Department of Homeland Security (DHS) Interagency Security Committee "Securing Government Assets through Combined Traditional Security and Information Technology" White Paper, issued in November 2013. These new requirements will have a transformational impact on the traditional building design, construction, operation and protection of building control systems and will require facility and information assurance professionals to learn building control system cyber skills.

COMMUNITY SEARCH

Enter search criteria...

LATEST NEWS [more](#)

10/7/2014 [Fourth Webinar in MMC's Series to Address Pressing Aspects of Hazard Mitigation](#)

10/6/2014 [LVDC Design Guidelines for the Visual Environment Available for Second Public Review](#)

10/2/2014 [Symposium Focuses on Helping Lead Communities to Higher Building Performance](#)

CALENDAR [more](#)

10/28/2014 - 10/30/2014 [ABX2014 - Architecture Boston Expo](#)

10/28/2014 [Sublandlading Mitigation—Florida's Less-Avoidance Assessment Strategy](#)

<http://www.nibs.org/news/166752/Institute-Workshops-to-Focus-on-Cybersecurity-of-Building-Control-Systems.htm>

QUESTIONS



**Michael Chipley
President, The PMC Group LLC
Cell: 571-232-3890
E-mail: mchipley@pmcgroup.biz**