Thank you for signing in early

The webinar will begin promptly at
12:00 pm ET, 9:00 am PT

SERDP DOD • EPA • DOE | ESTCP

SERDP and ESTCP Webinar Series

The webinar will begin promptly at 12:00 pm ET, 9:00 am PT

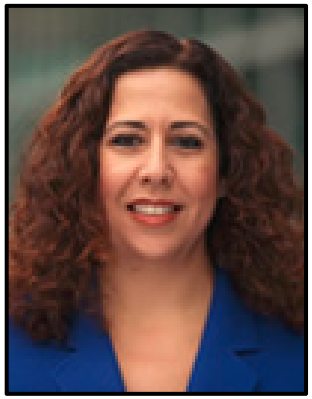
- You have two options for accessing the webinar
  1. Listen to the broadcast audio if your computer is equipped with speakers
  2. Call into the conference line: 303-248-0285
     Required conference ID: 6102000
- For any question or issues, please email serdp-estcp@noblis.org or call 571-372-6565

"Cyber Security and its Impacts on Installation Energy Management"

October 6, 2016

SERDP DOD • EPA • DOE | ESTCP

Welcome and Introductions



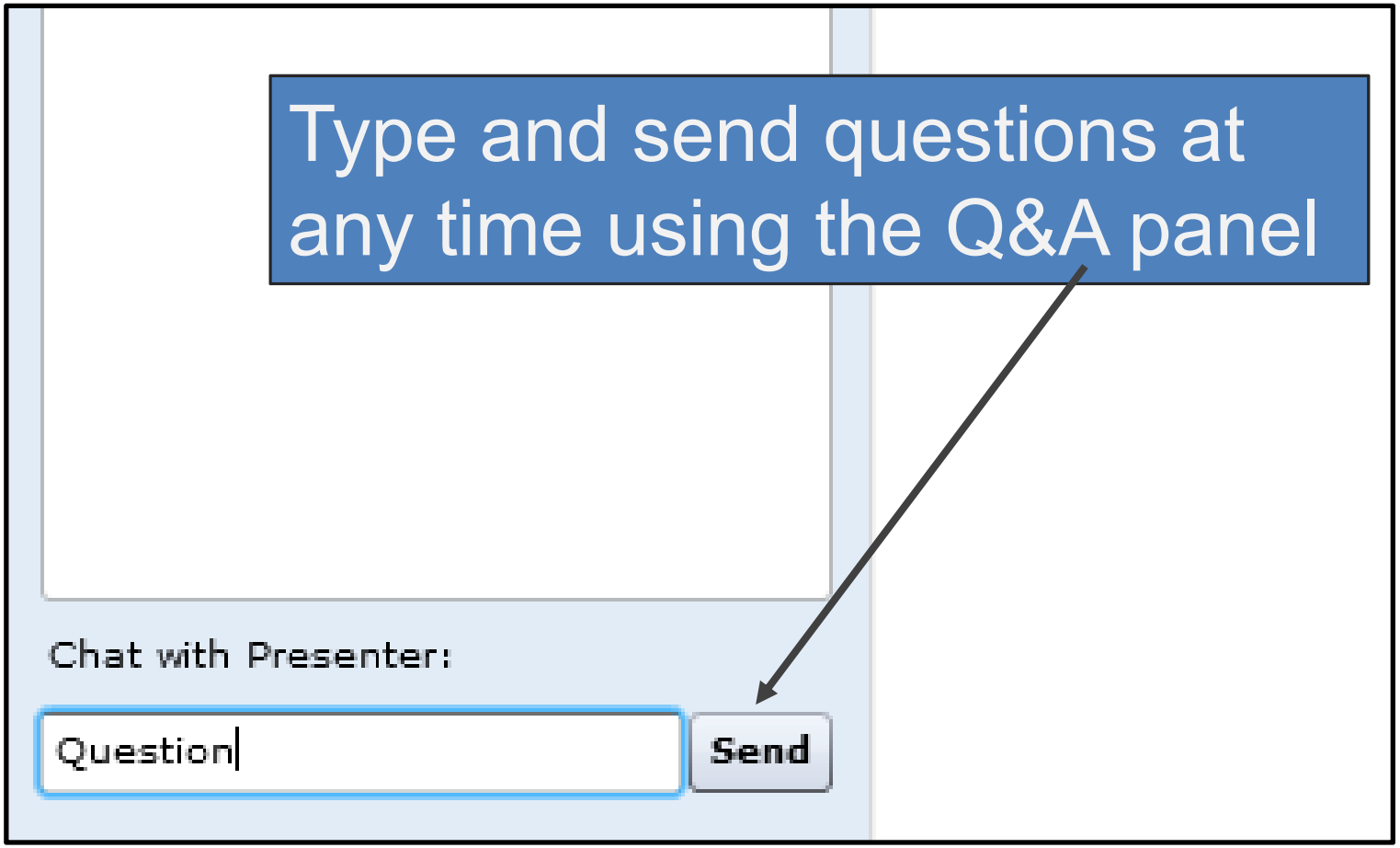
Rula A. Deeb, Ph.D.
Webinar Program Coordinator

SERDP DOD • EPA • DOE | ESTCP

Agenda

- **Webinar Logistics**
  Rula Deeb, Geosyntec Consultants (5 minutes)
- **Overview of SERDP and ESTCP**
  Timothy Tetreault, SERDP and ESTCP (5 minutes)
- **DoD Perspective on Cyber Security and its Impacts on Installation Energy Management**
  Dr. Michael Chipley, The PMC Group (17 minutes + Q&A)
- **Critical Energy Infrastructure Cyber Defense-in-Depth**
  Mr. Kevin Jordan, Resurgo (17 minutes + Q&A)
- **Cyber-Security Integrity for Electric Grid Facilities Management**
  Dr. Daniel Quinlan, LLNL (17 minutes + Q&A)
- **Final Q&A session**

How to Ask Questions



In Case of Technical Difficulties

- Delays in the broadcast audio
  - Click the mute/connect button
  - Wait 3-5 seconds
  - Click the mute/connect button again
  - If delays continue, call into the conference line
    - Call into the conference line: 303-248-0285
    - Required conference ID: 6102000
- Submit a question using the chat box

SERDP and ESTCP Overview

Timothy Tetreault
Energy and Water Program Manager

SERDP DOD • EPA • DOE | ESTCP

SERDP

Strategic Environmental Research and Development Program

- Established by Congress in FY 1991
  - DoD, DOE and EPA partnership
- SERDP is a requirements driven program which identifies high-priority environmental science and technology investment opportunities that address DoD requirements
  - Advanced technology development to address near term needs
  - Fundamental research to impact real world environmental management

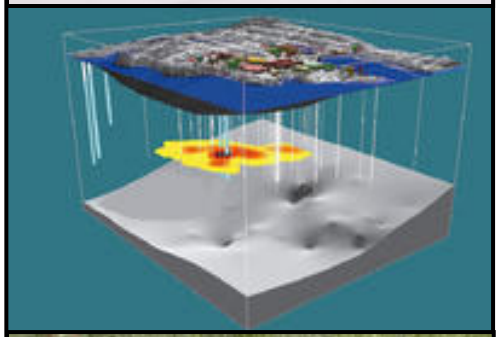
ESTCP

Environmental Security Technology Certification Program

- Demonstrate innovative cost-effective environmental and energy technologies
  - Capitalize on past investments
  - Transition technology out of the lab
- Promote implementation
  - Facilitate regulatory acceptance

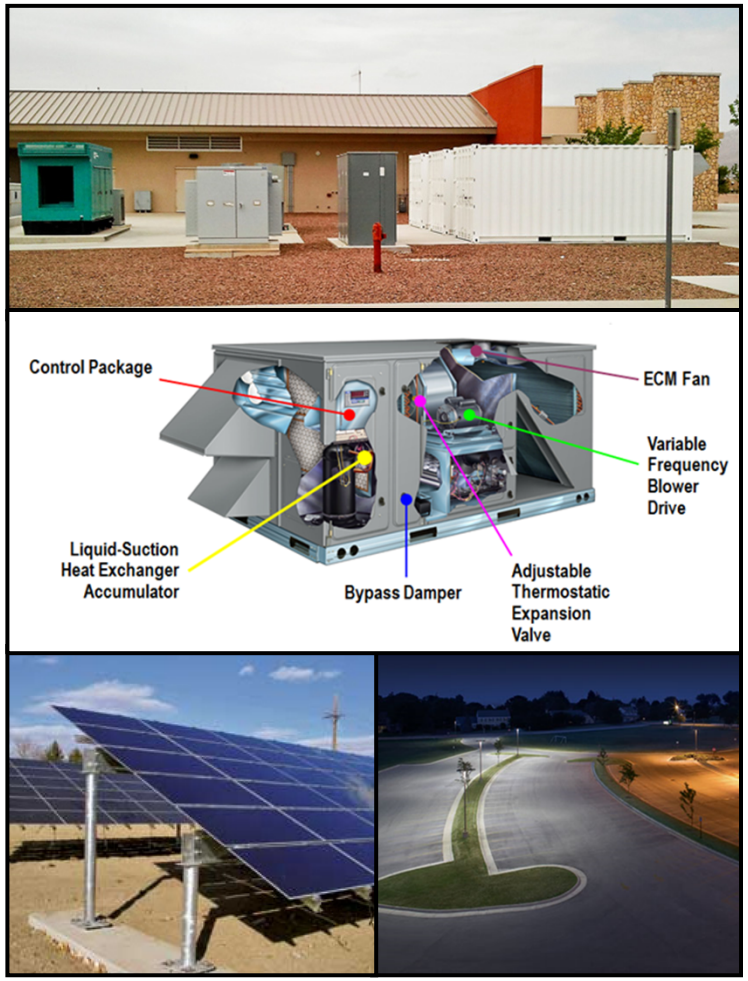
Program Areas

1. Energy and water
2. Environmental restoration
3. Munitions response
4. Resource conservation and climate change
5. Weapons systems and platforms



Energy and Water

- Smart and secure installation energy management
  - Microgrids
  - Energy storage
  - Ancillary service markets
- Efficient integrated buildings and components
  - Design, retrofit, operate
  - Enterprise optimized investment
  - Advanced components
  - Intelligent building management
  - Non-invasive energy audits
- Distributed generation
  - Cost effective
  - On-site
  - Emphasis on renewables



SERDP and ESTCP Webinar Series

Date	Topic
October 20, 2016	Resource Conservation and Climate Change “DoD Decision Making and Climate Change”
November 3, 2016	Environmental Restoration
November 17, 2016	Weapons Systems and Platforms
December 15, 2016	Environmental Restoration

SERDP and ESTCP Webinar Series

http://serdp-estcp.org/Tools-and-Training/Webinar-Series

SERDP
DOD • EPA • DOE

ESTCP

DoD Perspective on Cyber Security and its Impacts on Installation Energy Management

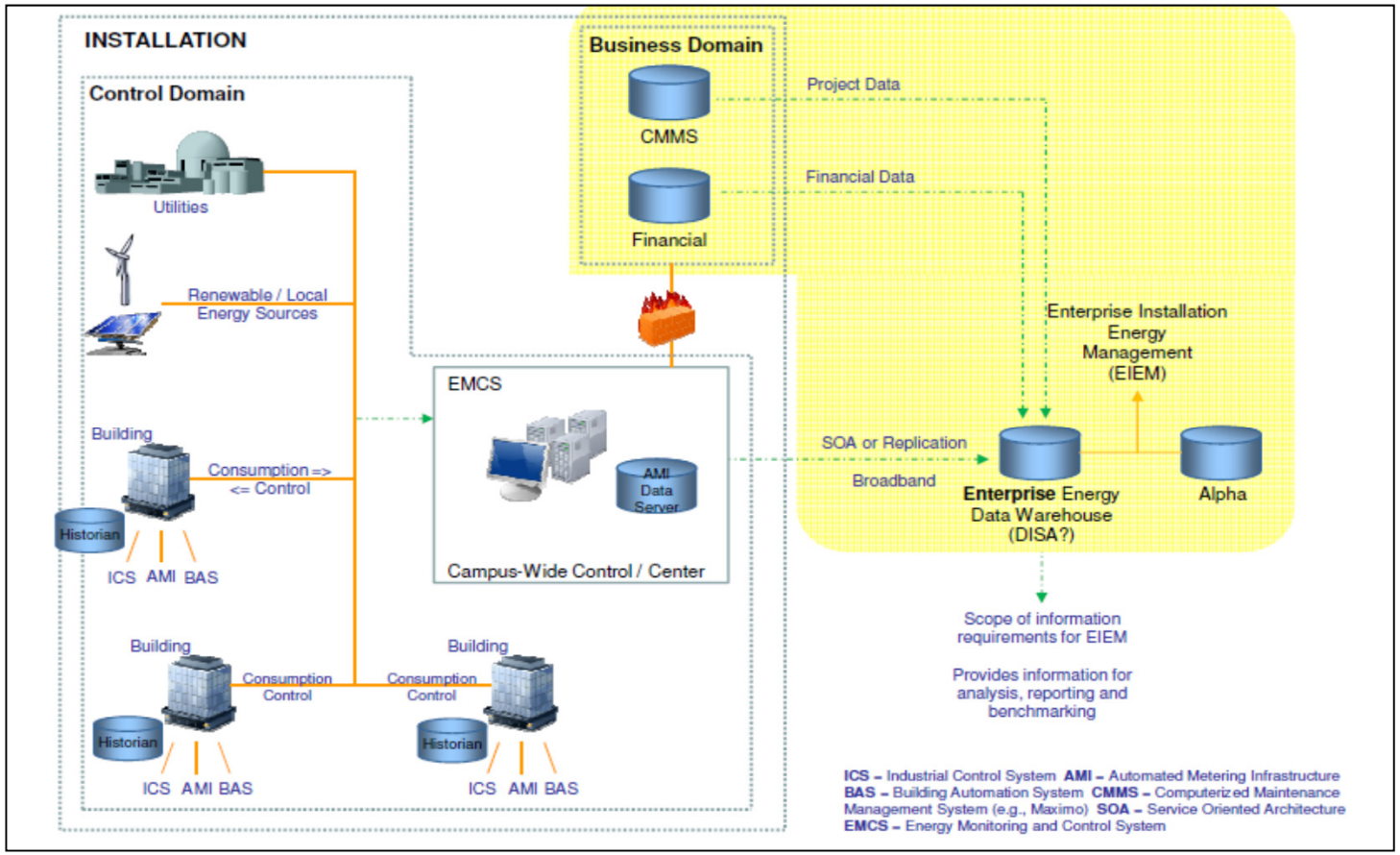
Dr. Michael Chipley
The PMC Group

SERDP DOD • EPA • DOE | ESTCP

Agenda

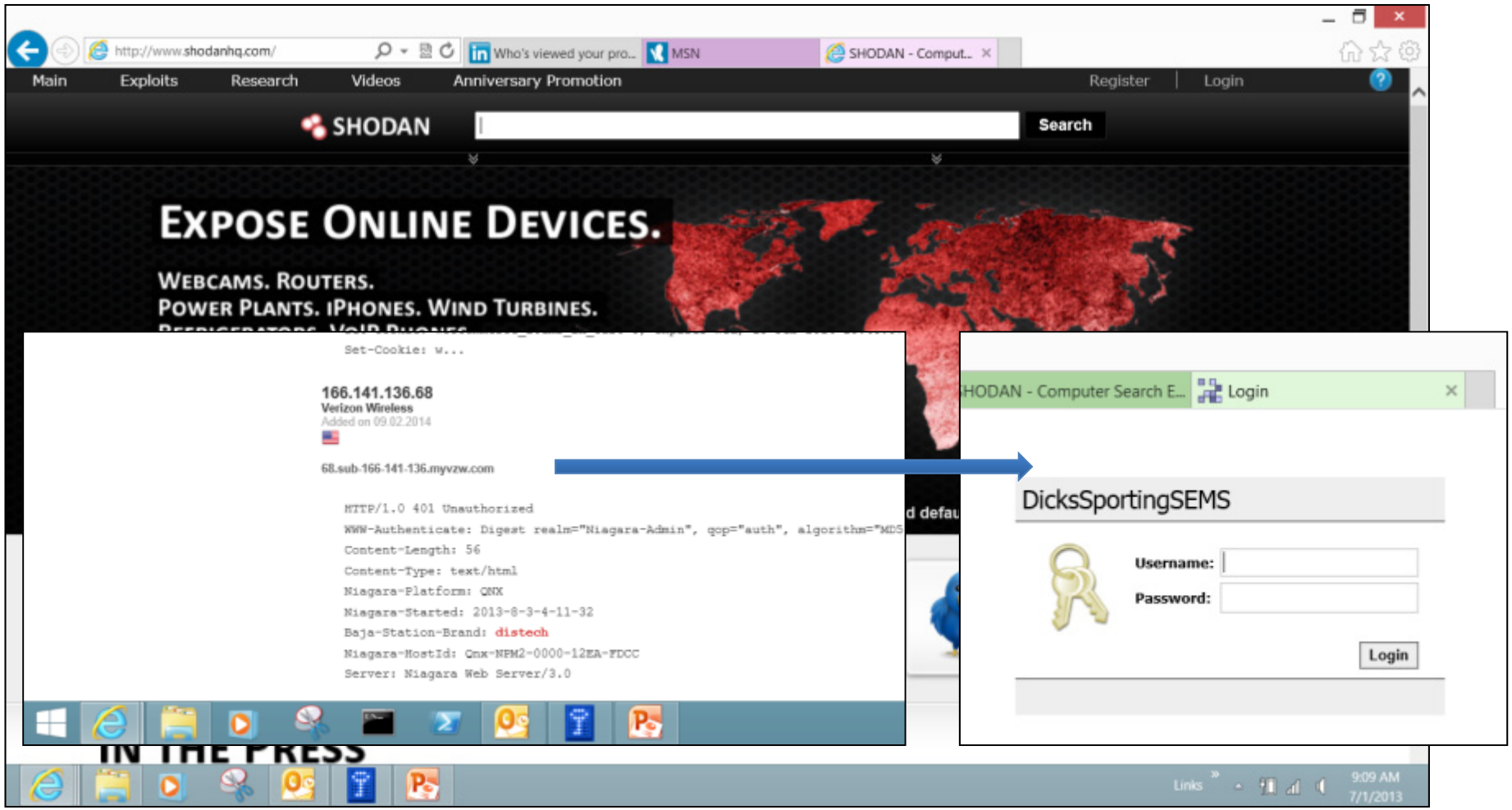
- How the DoD energy cyber program began
- DoD Risk Management Framework (RMF)
- Key resources and guidance
- Next steps
- ESTCP Subject Matter Expert (SME) support to project teams

In the Beginning…2010 Smart Installations



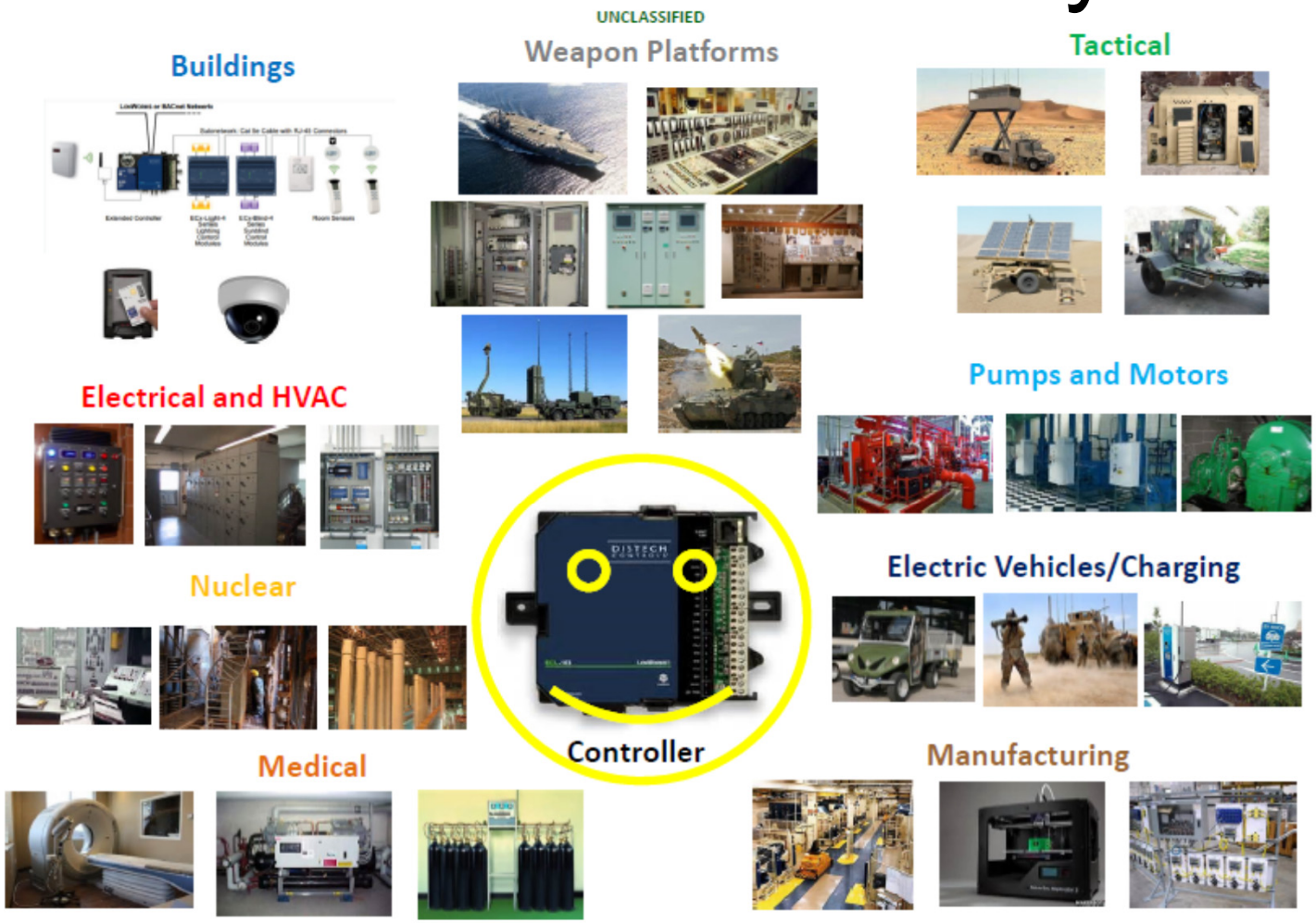
A great idea rudely interrupted by reality…Chief Information Officer (CIO) Advanced Meter Infrastructure (AMI) Authority To Operate (ATO) denial… and Stuxnet malware attack on Iranian Centrifuges

Shodan = Locates Control Systems (CS)



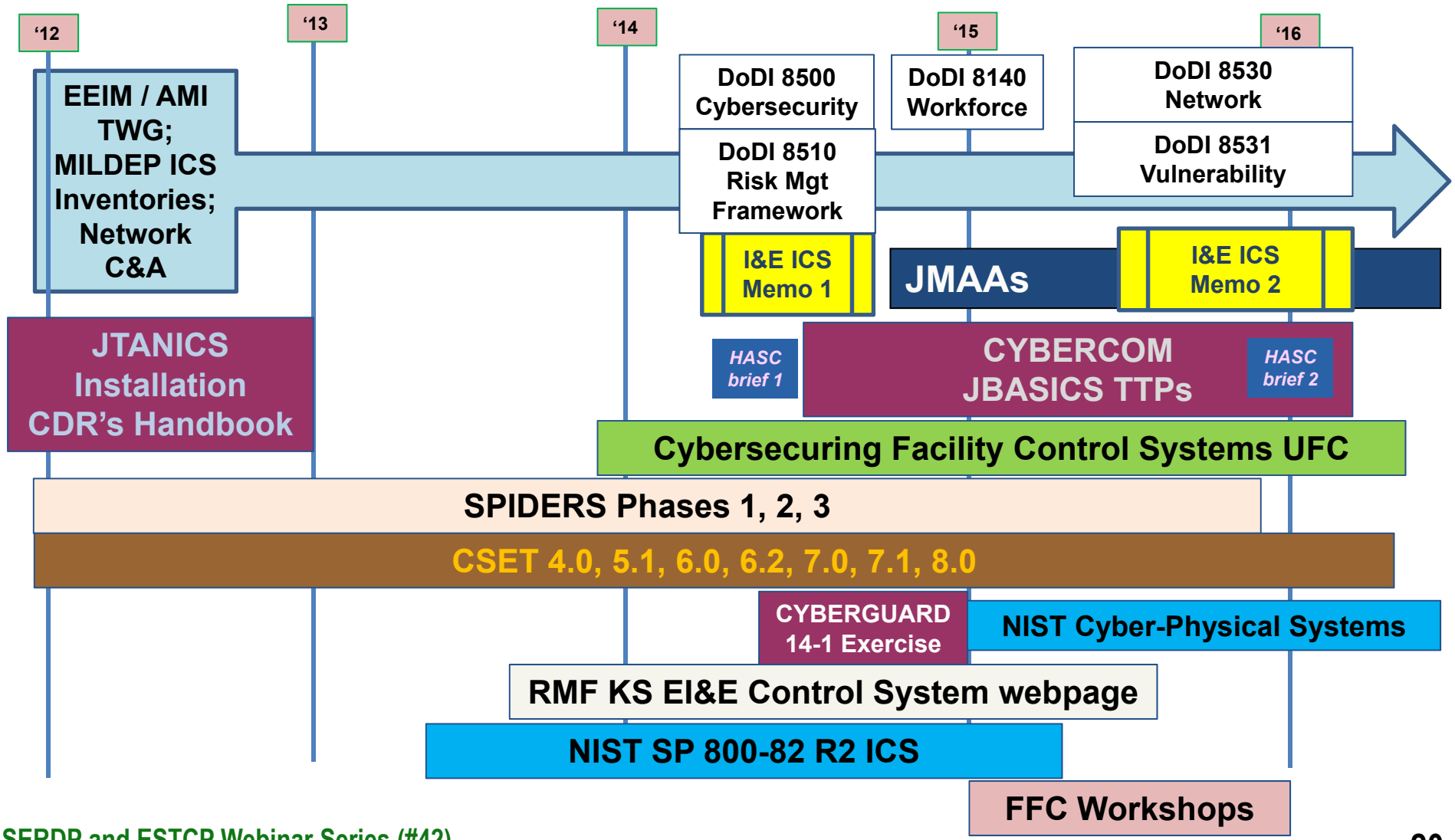
DoD has many CS systems directly connected to internet with no protection, http

OT IP Controllers are Everywhere

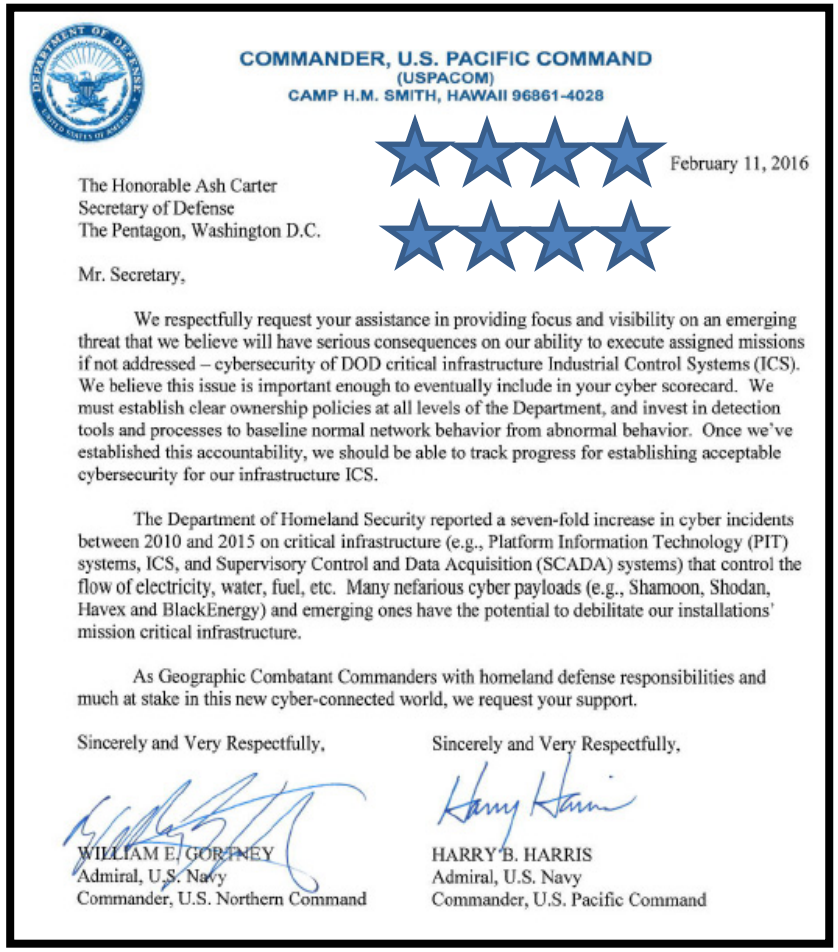


Same Commercial Device Installed Across DoD Enterprise; PIT & PIT Systems

Broader Cyber Security Efforts



“8 Star Memo”



COMMANDER, U.S. PACIFIC COMMAND
(USPACOM)
CAMP H.M. SMITH, HAWAII 96861-4028

February 11, 2016

The Honorable Ash Carter
Secretary of Defense
The Pentagon, Washington D.C.

Mr. Secretary,

We respectfully request your assistance in providing focus and visibility on an emerging threat that we believe will have serious consequences on our ability to execute assigned missions if not addressed – cybersecurity of DOD critical infrastructure Industrial Control Systems (ICS). We believe this issue is important enough to eventually include in your cyber scorecard. We must establish clear ownership policies at all levels of the Department, and invest in detection tools and processes to baseline normal network behavior from abnormal behavior. Once we've established this accountability, we should be able to track progress for establishing acceptable cybersecurity for our infrastructure ICS.

The Department of Homeland Security reported a seven-fold increase in cyber incidents between 2010 and 2015 on critical infrastructure (e.g., Platform Information Technology (PIT) systems, ICS, and Supervisory Control and Data Acquisition (SCADA) systems) that control the flow of electricity, water, fuel, etc. Many nefarious cyber payloads (e.g., Shamoon, Shodan, Havex and BlackEnergy) and emerging ones have the potential to debilitate our installations' mission critical infrastructure.

As Geographic Combatant Commanders with homeland defense responsibilities and much at stake in this new cyber-connected world, we request your support.

Sincerely and Very Respectfully,

WILLIAM E. GORTNEY
Admiral, U.S. Navy
Commander, U.S. Northern Command

Sincerely and Very Respectfully,

HARRY B. HARRIS
Admiral, U.S. Navy
Commander, U.S. Pacific Command

- Establish clear ownership
- Include in Scorecard
- Invest in detection tools
- Seven times cyber incidents

NDAA 2017

- DoD facilities transitioning to smart buildings; increased connectivity has increased threat and vulnerability to cyber-attacks. Therefore, SECDEF deliver a report:
  1. Identify structural risks inherent in control systems and networks
  2. Assess the current vulnerabilities to cyber attack initiated through Control Systems (CS) at DoD installations worldwide
  3. Propose a common, DoD-wide implementation plan
  4. Require the consideration of cybersecurity vulnerabilities and cyber risk in preconstruction design processes and requirements development processes for military construction projects
  5. Identify and mitigate full-spectrum cyber-enabled risk to new facilities and major renovations

DoDI 8500.01 PIT Examples

Vehicles and alternative fueled vehicles (e.g., electric, bio-fuel, Liquid Natural Gas that contain car-computers), buildings and their associated control systems (building automation systems or building management systems, energy management system, fire and life safety, physical security, elevators, etc.), utility distribution systems (such as electric, water, waste water, natural gas and steam), telecommunications systems designed specifically for industrial control systems including supervisory control and data acquisition, direct digital control, programmable logic controllers, other control devices and advanced metering or sub-metering, including associated data transport mechanisms (e.g., data links, dedicated networks)

Installations and Environment worked with CIO to expand definition of PIT systems, then added to NIST SP 800-82R2 – 3 years in the making

DoDI 8530 DoDIN

Department of Defense
INSTRUCTION

NUMBER 8530.01
March 7, 2016

DoD CIO

SUBJECT: Cybersecurity Activities Support to DoD Information Network Operations

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Directive (DoDD) 5144.02 (Reference (a)), this instruction:

a. Reissues DoDD O-8530.1 (Reference (b)) as a DoD Instruction (DoDI) and incorporates and cancels DoDI O-8530.2 (Reference (c)) to establish policy and assign responsibilities to protect the Department of Defense information network (DoDIN) against unauthorized activity, vulnerabilities, or threats.

b. Supports the Joint Information Environment (JIE) concepts as outlined in JIE Operations Concept of Operations (CONOPS) (Reference (d)).

c. Supports the formation of Cyber Mission Forces (CMF), development of the Cyber Force Concept of Operations and Employment, evolution of cyber command and control, cyberspace operations doctrine in Joint Publication 3-12 (Reference (e)), and evolving cyber threats.

d. Supports the Risk Management Framework (RMF) requirements to monitor security controls continuously, determine the security impact of changes to the DoDIN and operational environment, and conduct remediation actions as described in DoDI 8510.01 (Reference (f).

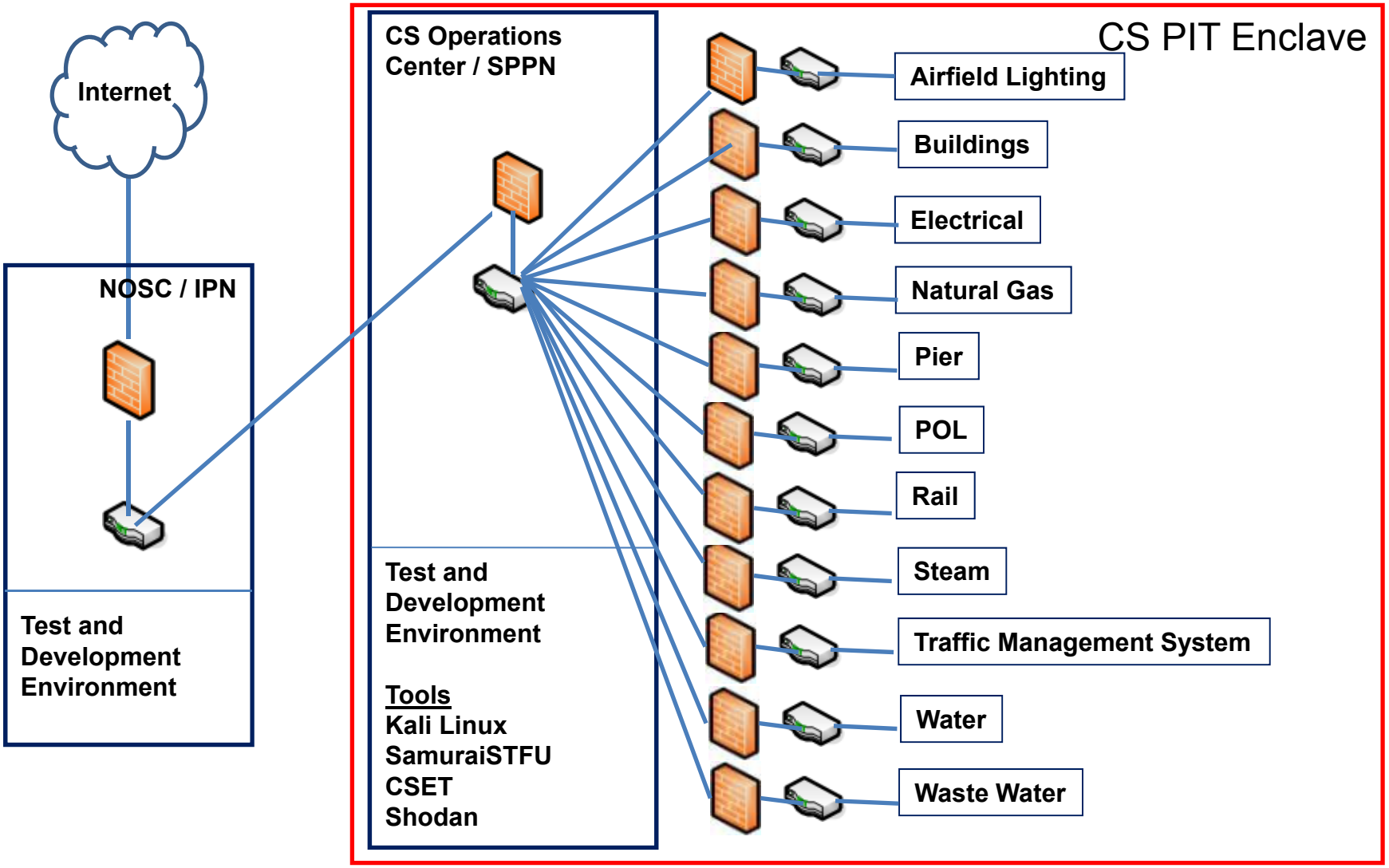
e. Cancels Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Memorandum (Reference (g)).

2. APPLICABILITY. This instruction:

a. Applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense (IG DoD), the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the "DoD Components").

- Control systems and industrial control systems (ICS) as defined in National Institute (NIST) Special Publication (SP) 800-82 that are owned or operated by or on behalf of DoD Components
- Joint Information Environment
  - Installation Processing Nodes (IPN)
  - Special Purpose Processing Nodes (SPPN)
  - Tactical Processing Nodes (TPN)

DoD CS Systems and the JIE

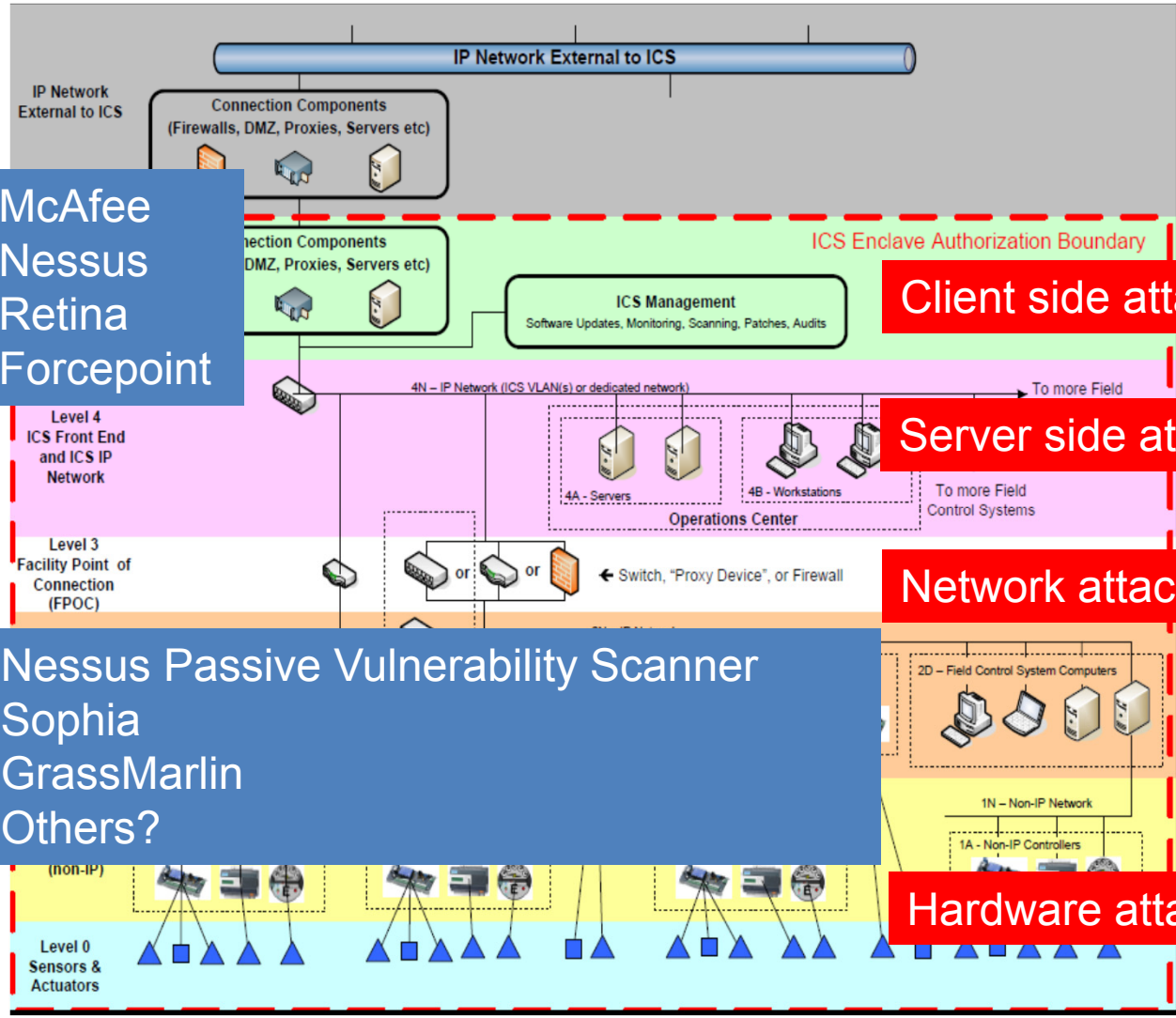


Continuous Monitoring and Attack Surfaces

Host based security systems
Scanning (Active)

Windows, Linux
HTTP, TCP, UDP

Intrusion detection systems (Passive)
PLC, RTU, Sensor
Modbus, LonTalk, BACnet, DNP3



McAfee
Nessus
Retina
Forcepoint

Client side attacks

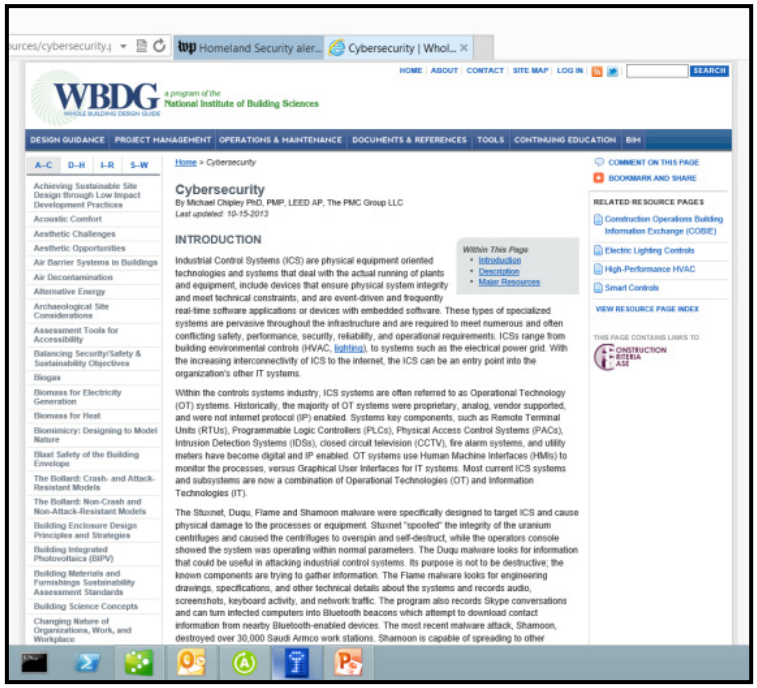
Server side attacks

Network attacks

Nessus Passive Vulnerability Scanner
Sophia
GrassMarlin
Others?

Hardware attacks

EI&E Cyber Resources

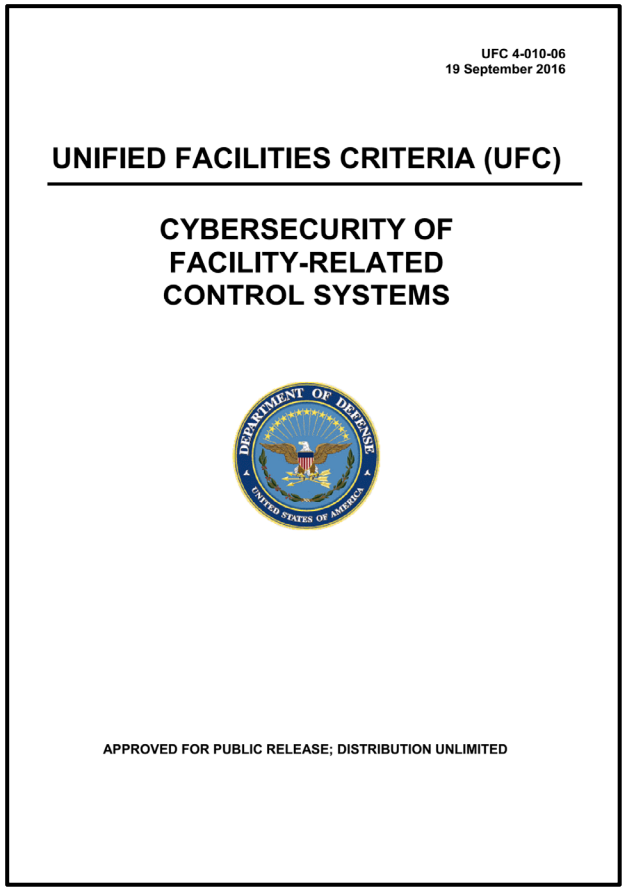


http://www.wbdg.org/resources/cybersecurity.php

Navigate to DoD CIO Knowledge Service (requires CAC) https://rmfks.osd.mil/login.htm

UFC 4-010-06 Cybersecurity of Facility-Related Control Systems

- This UFC provides criteria for the inclusion of cybersecurity in the design of control systems in order to address appropriate Risk Management Framework (RMF) security controls during design and subsequent construction
- Historically, control systems have not included these cybersecurity requirements, so the addition of these cybersecurity requirements will increase both cost and security

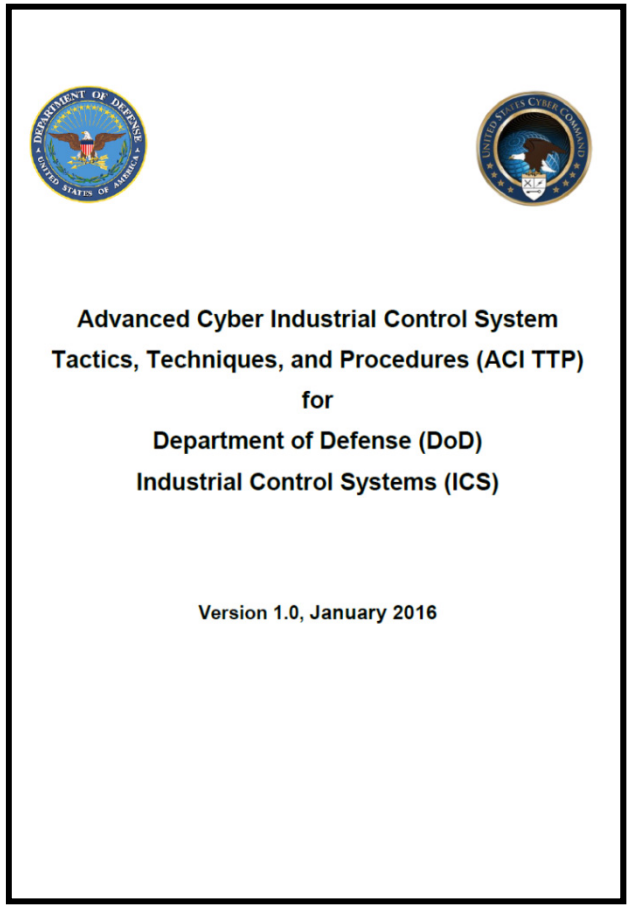

UFC 4-010-06
19 September 2016

UNIFIED FACILITIES CRITERIA (UFC)

CYBERSECURITY OF FACILITY-RELATED CONTROL SYSTEMS

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

ACT TTP for DoD ICS


Advanced Cyber Industrial Control System
Tactics, Techniques, and Procedures (ACI TTP)
for
Department of Defense (DoD)
Industrial Control Systems (ICS)

Version 1.0, January 2016

How to Use TTPs

This ACI TTP is divided into essentially four sections:

- **ACI TTP Concepts** (chapters 2 through 4)
- **Threat-Response Procedures** (**Detection, Mitigation, Recovery**) (enclosures A, B, and C)
- **Routine Monitoring of the Network and Baselining the Network** (enclosures D and E)
- **Reference Materials** (enclosures F through I and appendix A through D)

Draft Navy BUMED IA Design Guidance

1.5 REQUIRED SUBMITTALS

The Contractor(s) shall develop and upload into the DoD CIO eMASS tool, all required artifacts and supporting documentation. This effort should result in the creation of an Authority To Operate (ATO) package. The required artifacts are determined by the system security classification, system categorization, and cybersecurity controls. This information may include but is not limited to the list below:

a. System Security Plan (SSP)
b. Configuration Management Plan (CMP)
c. Disaster Recovery Plan (DRP)
d. Continuity of Operations (COP)
e. Information Technology Contingency Plan (ITCP)
f. Incidence Response Plan (IRP)
g. Security Assessment Report (SAR)
h. Plan of Action and Milestones (POAM)
i. System Architecture/Topology/Data Flow
j. Configuration Validation Checklist
k. Security Classification Guide
l. System Configuration Guide
m. Hardware Inventory List
n. Software Inventory List
o. Physical Security Plan
p. Personnel Security Plan
q. Information Assurance Vulnerability Management
r. Patch Management Process, Connection Approval
s. Ports, Protocols, and Services (PPS) List
t. Active Directory (AD) Documentation, (if applicable)
u. Jump-Kit Rescue CD

1.10 TEST AND DEVELOPMENT ENVIRONMENT The Systems Integrator will establish a Test and Development Environment (TDE) that replicates the Production Environment to the highest degree possible starting with the Level 4 Workstations, Servers, BAS software and with at least one of each of the Level 3-0 major components, devices, and actuators.

At approximately the 50-75% construction complete, the TDE will be used to perform Factory Acceptance Testing (FAT) of the BAS to ensure the BAS has end-to-end functionality, has been properly configured using the Security Content Automation Protocol (SCAP) tool and the Security Technical

Utility Monitoring and Control System Engineering Requirements Manual **Navy Medicine West**

(Both hardware and software/firmware lists should also include Common Criteria EAL status, DADMS entry number, and OS/IOS/Firmware version(s) as applicable).

- Network diagram
  - Network diagram must show equipment locations, names, models, and IP addresses on network communications schematic.
- Jump-Kit Rescue CD
  - The Rescue CD is a bootable CD with tools, rootkit detection, master boot record check, and other capabilities. A Recovery Jump-Kit contains the tools the ICS team and IT team will need to restore a system to its last FMC state during Mitigation and Recovery. The Jump-Kits must be maintained and be a part of configuration management. When configuration files or new versions of operating systems or applications are updated, the Jump-Kits need to be updated as well.

TTP Jump-Kit Rescue CD

What's Next?

- DoD CIO Control Systems Scorecard Fall 2016
- Platform Resilience Mission Assurance effort starts Spring 2016
- JHU-APL Cyber Threats, Gaps, Workforce Reports Fall 2016
- Cyber Ranges Control Systems Competition 2017
- Acquisition and contract language to require contractors and vendors IT Business Systems to meet DoD standards (NIST SP 800-171) per DFAR 2015 – Compliance Date: Dec 2017

Conclusions

- All control system projects must follow the RMF process – design cyber in from the beginning
- The CIO RMF KS Portal EI&E webpage provides general guidance and resources
- The new UFC and TTP's provide detailed guidance and required deliverables (but not all will apply to every project)
- ESTCP office will provide SME support to project teams to complete RMF packages

For additional information, please visit
https://serdp-estcp.org/

Speaker Contact Information

mchipley@pmcgroup.biz; 571-232-3890

Q&A Session 1

SERDP DOD • EPA • DOE | ESTCP

Cyber Security of Control Systems and its Impacts on Installation Energy Management

Kevin B. Jordan
Resurgo

SERDP DOD • EPA • DOE | ESTCP

Problem Statement

- The DOD lacks the ability to defend the industrial control systems of Posts, Bases, Camps, Installations and related civilian critical energy infrastructure against cyber-attacks from nation state actors and Advanced Persistent Threats (APT)
- Current Industrial Control System (ICS) defense "Code of Best Practices" approach is based on erroneous assumptions
  - "Air gapped" from the Internet status can be maintained
  - Fully "patched and up-to-date" system status can be achieved
- Shortcomings to the current approach
  - Remote access to protected networks introduces vulnerabilities
  - Age and uniqueness of systems sometimes preclude patching and updating
  - Anti-virus and anti-malware protection only effective against previously identified attacks
  - The best "best practices" defense deteriorates over time

The Solution – An ESTCP Project

- **Project objective**: *Successfully demonstrate a Fault and Intrusion Tolerant Cyber-secure defense-in-depth of an electrical power plant against attacks representative of Tier V/Nation-state actors*
  - Demonstrate to DoD and commercial energy providers a new capability to mitigate and recover quickly from online and insider cyber activities directed against SCADA (Supervisory Control and Data Acquisition) infrastructure
- Fault and intrusion tolerant focus
- Show new technologies employed in a defense-in-depth configuration to enable a utility's control system to "fight through" an attack without disruption of services
- Improve current methodology and best practices
- Set new guidelines and techniques for capitalizing on emerging technologies and processes tested by the Defense Advanced Research Projects Agency (DARPA) and the Director, Operational Test and Evaluation (DOT&E)

Why Defend Commercial Power?

- All DoD installations in Hawaii rely on power from "outside the wire"/public utility power
- ESTCP funded a Public-Private partnership [DoD-DOE-Utility Company-Industry] to demonstrate an approach to cyber secure critical power utility control systems supporting the U.S. Pacific Command (PACOM)
- Five technologies constitute layered defense from the Internet to the generator
- Defense-in-depth harder to penetrate than single line of defense

Our Defense is Fault Tolerant

- Fault tolerance is the ability to continue to function despite physical network problems (i.e., fiber seeking backhoe or Murphy)
- Fault tolerance ensures continuity of communications between the human and the device
- Critical communications continue so long as a physical path exists
- Fault tolerant systems are resilient and assure power availability

Our Defense is Intrusion Tolerant

- Intrusion tolerance is the ability to continue the mission despite APT presence in the network
- Critical functionality can NOT be knocked offline
  - Power continues to flow to DoD customers (availability)
  - Critical C2 (command and control) nodes continue to operate
- Intrusion tolerant systems handle the threat and assure power availability

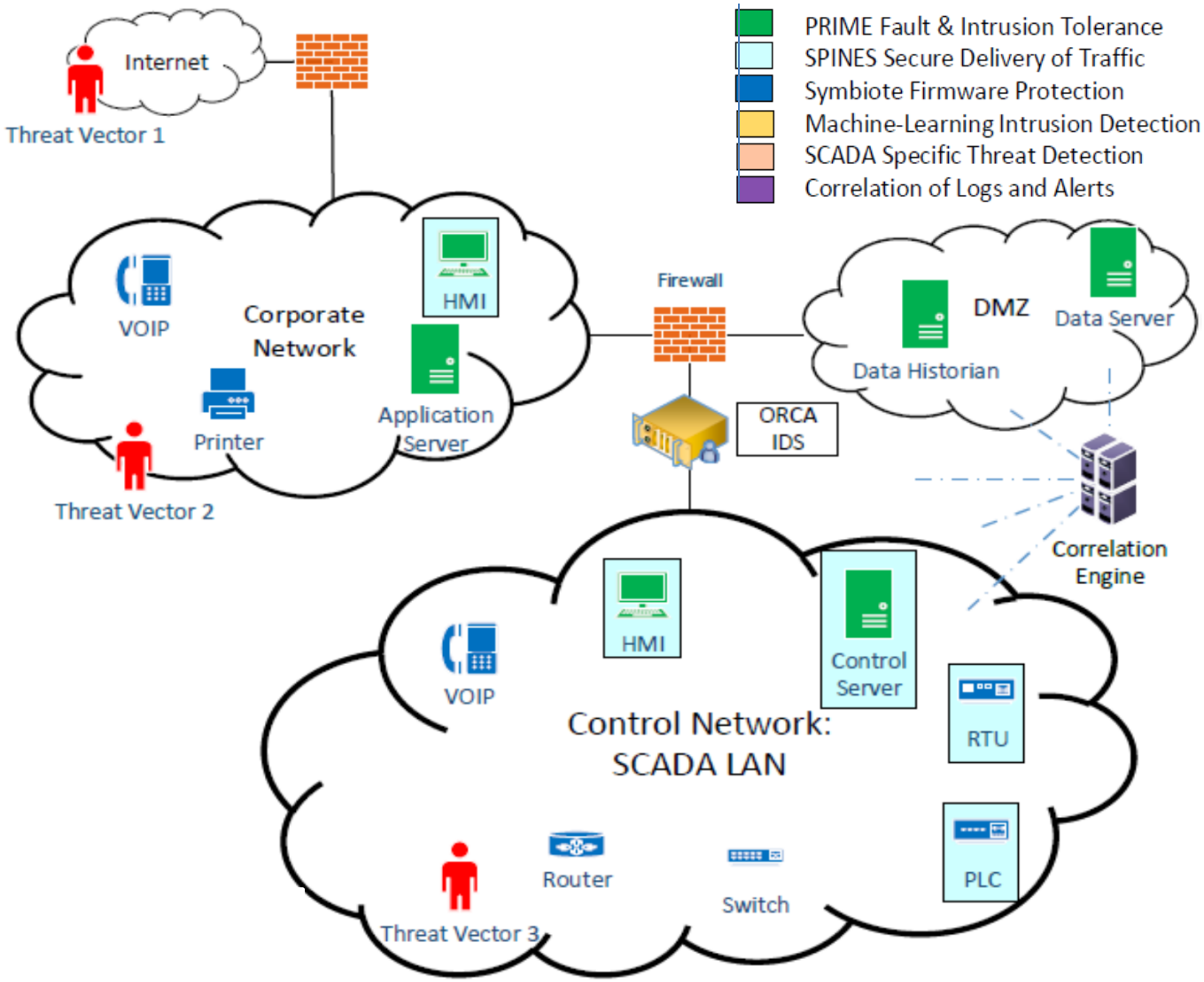
Cyber protected power assures the mission!

Technology Overview

Four technologies, layered in a defense-in-depth and reporting to a SIEM (Security Information and Event Management)

- Machine-learning sensor
  - Trained and focused on network behavior and information flows
- Spines (overlay communications architecture)
  - Ensures fault tolerant delivery of control system traffic within tight time constraints while blocking adversary positioning for man-in-the-middle-attacks
- Prime (multi-compiler)
  - An intrusion-tolerant replication of Supervisory Control And Data Acquisition (SCADA) Master
  - Prevents attackers from disrupting the replicated critical ICS functions
  - Each replication presents a different attack surface (different variation)
- Symbiote (end-point security wrapper)
  - Protects Remote Terminal Units (RTU), Programmable Logic Controllers (PLCs), printers and Voice Over Internet Protocol (VOIP) phones
  - Merges with device firmware to form a unique binary that permits legitimate updates to firmware while preventing unauthorized changes

Operational Network View



Potential Technology Transition Path

- Dual transition paths
  - The DoD, led by NAVFAC Engineering Expeditionary Warfare Center (EXWC), see potential use at Joint Base Pearl Harbor Hickam and other Pacific bases
  - The commercial sector, led by Pacific Northwest National Lab with ourupartner
- Shared across DoD immediately
- NIST (National Institute for Standards) shares actionable cyber security information with industry
- FBI “InfraGard” program shares information across the defense industrial base

Acknowledgments

- USPACOM Energy Innovation Office
- DARPA I20 MRC/CRASH Program
- NAVFAC N6

For additional information, please visit
https://serdp-estcp.org/Program-Areas/Energy-and-Water/Energy/Microgrids-and-Storage/EW-201607

Speaker Contact Information

kevin.b.jordan@resurgo.net; 808-425-5324

SERDP DOD • EPA • DOE | ESTCP

Q&A Session 2

SERDP DOD • EPA • DOE | ESTCP

Cyber-Security Integrity for Electric Grid Facilities Management

Dr. Daniel Quinlan
Lawrence Livermore National Laboratory

LLNL-PRES-704260
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Problem Statement

Challenge

- Cyber attacks on energy management devices and systems could significantly impact military operations at DoD bases
- Insertion of vulnerabilities and malware via updates/upgrades of control system software (i.e., firmware) is a known cyber attack vector
- Software development errors can result in cyber vulnerabilities in firmware similar to other software

Shortcomings of current approach

- Vendors will apply some level of secure code development, but cannot detect supply chain attacks in either libraries, where source code is unavailable, or on route to a facility
- Identification of vulnerabilities and malware in firmware is rarely performed at facility due to expense and expertise required
- There exist no automated tools for use by field engineers to test firmware

Technical Objectives

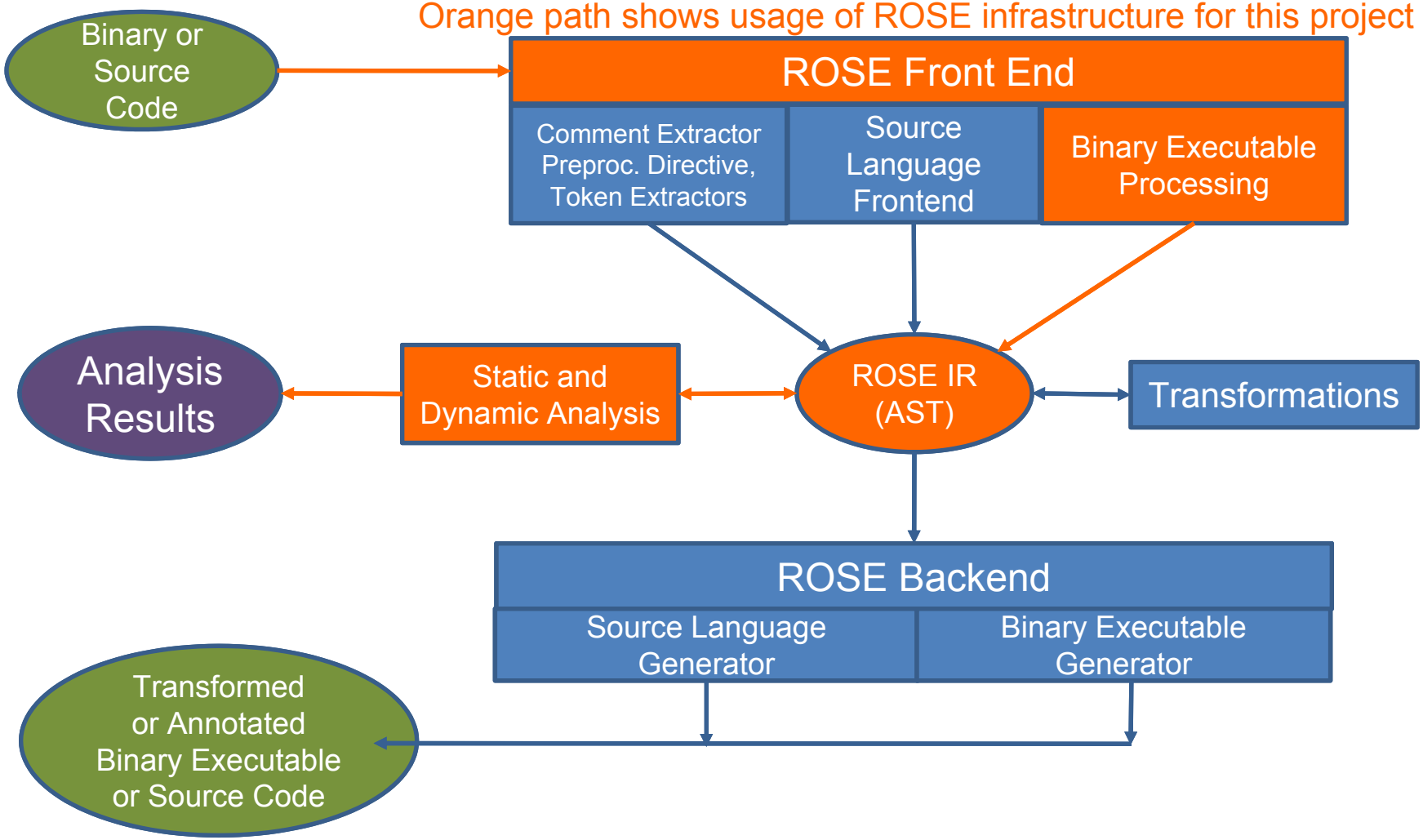
- Define a process to mitigate the risk of malware and vulnerabilities in binary firmware updates using specific tools
- Make existing binary analysis tools for firmware analysis more robust
- Test and evaluate technology in testbeds and at DoD installation
- Define how to integrate tool use into the maintenance of electric grid substations and building automation systems
- Define how to integrate firmware analysis tools within security assessments of DoD base infrastructure
- Improve security best practices

ROSE Technology Description

- Technology
  - Binary Analysis Tools (BATs) developed under Supply Chain Integration For Integrity (SCI-FI) and the tool infrastructure (ROSE) used to build them
  - ROSE provides a base level of technology for our tools
    - Disassembly of binary executables (firmware)
    - Numerous forms of pre-packaged analysis
    - Presentation of analysis results
    - Building custom analysis tools
  - ROSE is unique and innovative
    - An open source infrastructure for software (source code and binaries) analysis (developed and applied for over 15+ years)
    - Provides mixed static and dynamic analysis using emulation
    - Complete representation of binary executable critical for malware analysis
    - Backup slide lists summary of ROSE binary analysis features
- Methodology
  - Focus on specific prototype firmware analysis tools developed for the DOE SCI-FI project for Supply Chain Integrity for the electric grid
  - Improve robustness and usability these tools on more firmware samples

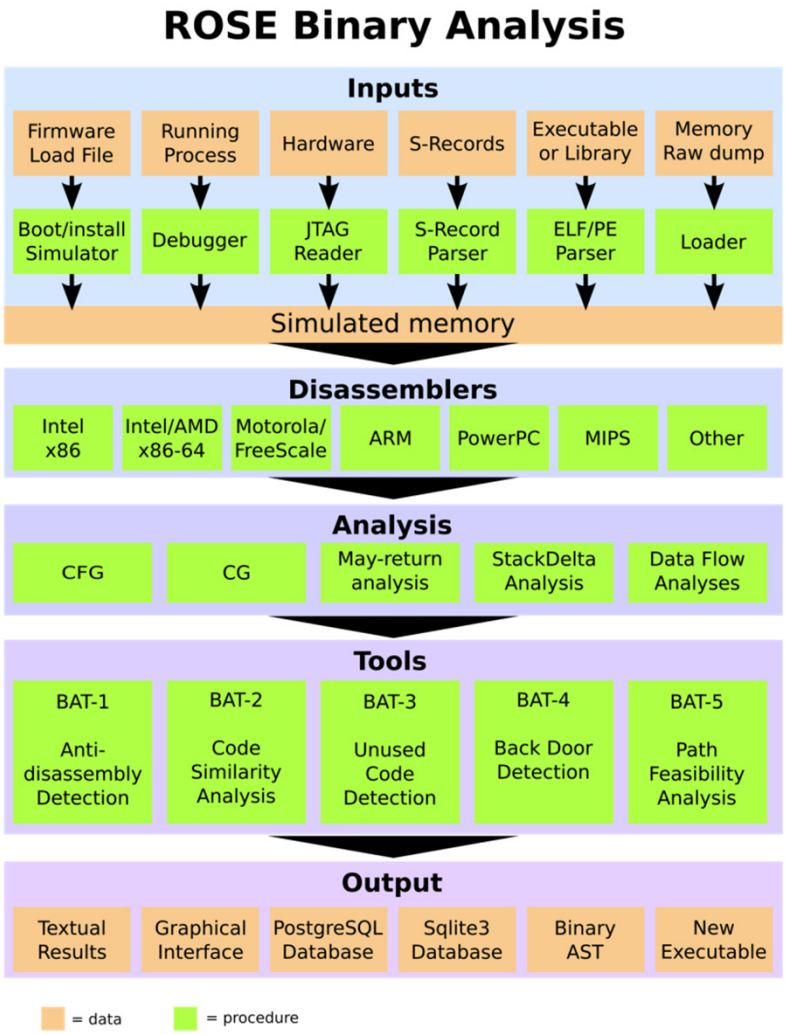
ROSE's Extensible Architecture Used to Develop Targeted Binary Analysis

Orange path shows usage of ROSE infrastructure for this project



Project will Adapt SCI-FI Tools Built on ROSE Framework

- Multiple inputs can drive firmware analysis
- Many kinds of Instruction Set Architectures (ISAs) are supported
- Tools are built from numerous forms of analysis
- Many capabilities in ROSE can be used to support analysis
- ROSE is an infrastructure for building firmware tools (BATs built for SCI-FI)
- Output can be presented many different ways



ROSE Technology History

ROSE technology has been in development for over 15 years and is being used for a wide variety of national security and science missions

- Mission applications
  - Software Engineering Institute (US CERT) building malware analysis tools for DoD and DHS
  - DOE program specific software analysis
  - DOE Nuclear stockpile stewardship software analysis and optimization
- Advanced demonstrations for IT
  - Vulnerabilities in sendmail, used as for email world-wide (binary analysis)
  - Vulnerabilities in hundreds of Linux utilities (binary analysis)
  - Vulnerabilities in Xen, Amazon cloud infrastructure (source code)
- ROSE has won numerous awards
  - 2009 R&D 100 award
  - Rigorous Examination of Reactive Systems (RERS) Software Analysis Challenges 2012, 2013, 2014, and 2015 awards

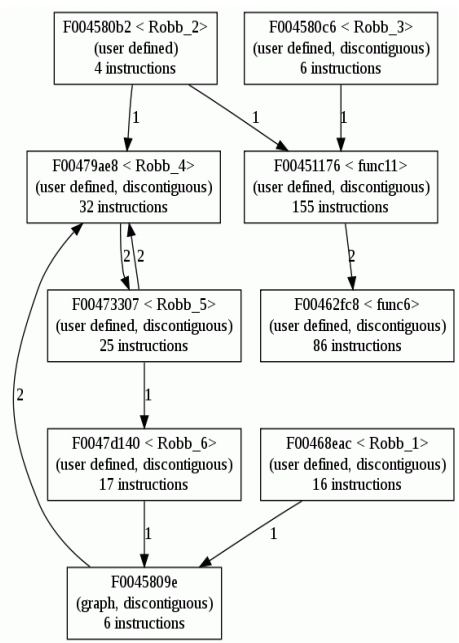
ROSE Technology for DoD

- SCI-FI tools demonstrations for grid devices
  - malware via associate with anti-disassembly techniques (binary analysis)
  - Backdoor analysis on sample codes
  - Identify specific properties (analysis results) on firmware
  - Most of the tools we developed, as well as the ROSE framework for building tools, are available open-source from www.rosecompiler.org
- Development work for DoD demonstration
  - Improve robustness of prototype SCI-FI tools to suit different types of users
  - Providing tool interfaces for different types of users
  - Testing and evaluation expanded to testbeds
  - Using firmware gathered from more devices
  - Communicating results to users and vendors to understand detected properties

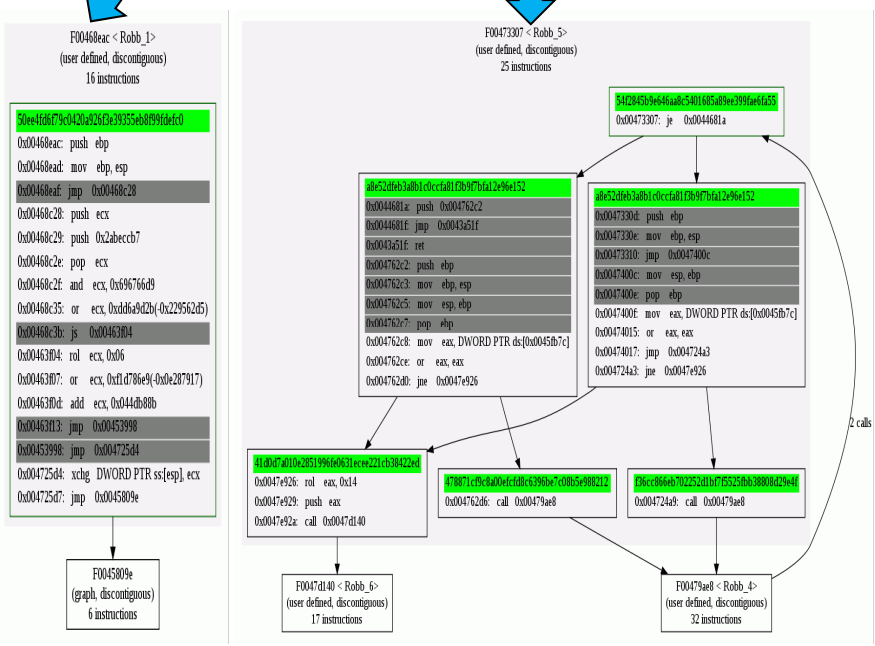
Detection of Anti-Disassembly Technology in Firmware (BAT-1)

- Funded under DOE SCI-FI project
- No Operation (NOP) equivalence regions detected *(gray)*
- Hash of the blocks semantics is generated *(green)*
- Binary transformations can rewrite these sections to be more clear within later phases of analysis

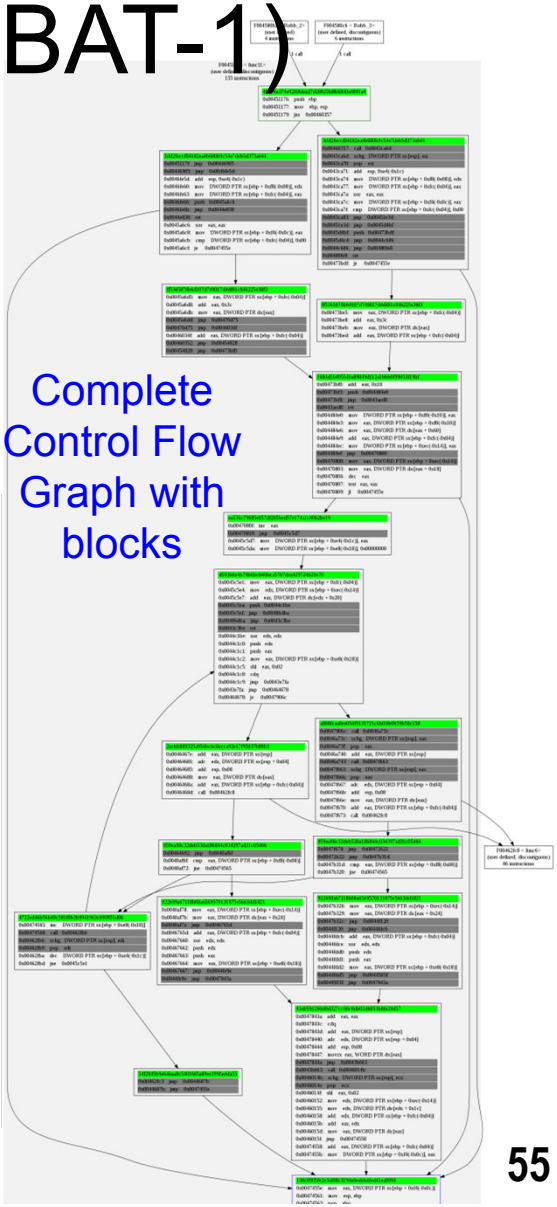
Function Call Graph



Separate Functions

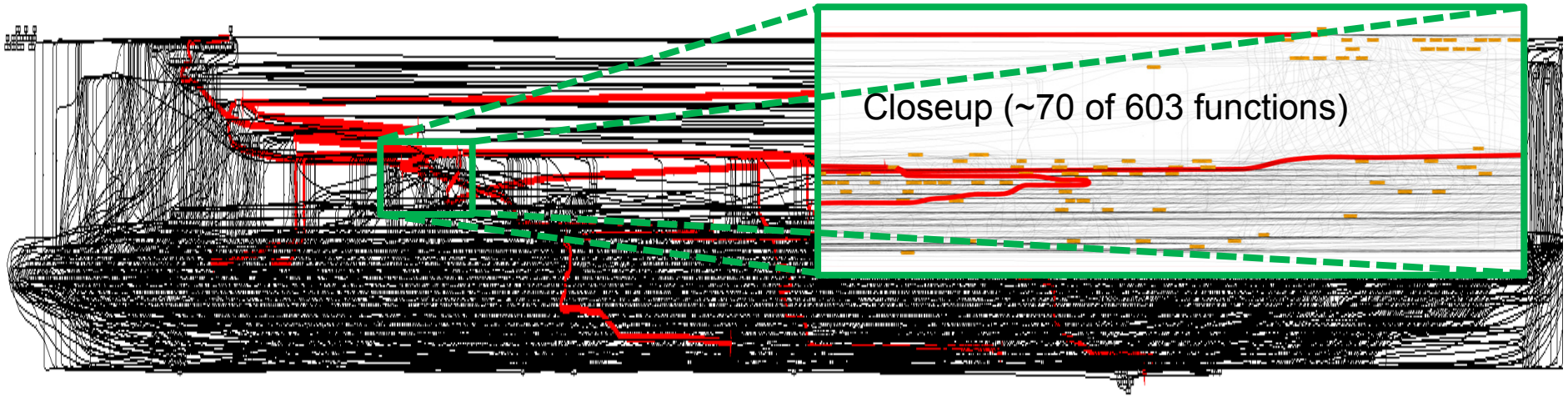


Complete Control Flow Graph with blocks



Async-Safe Signal Handler Vulnerability (BAT-5)

- Funded by internal LLNL research
- Call graph shows 603 functions 2888 function calls
- Found vulnerability in binary of *sendmail* utility
- Some paths through the control flow have errors *(one path shown in red)*
- Reported to *sendmail* developers
- Also used to automate testing for vulnerability in hundreds of Linux utilities



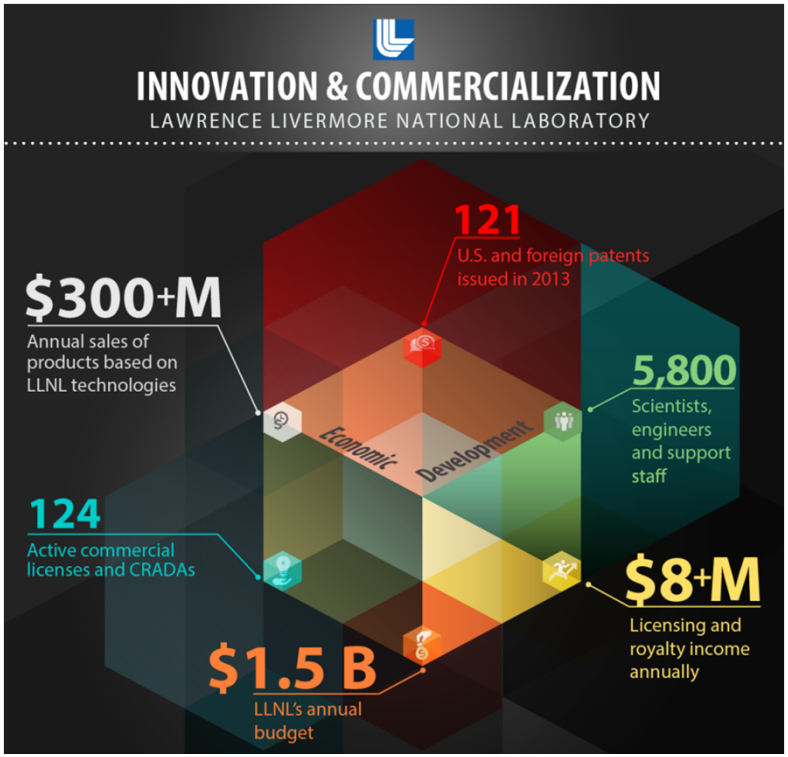
Call Graph for *sendmail* program (computed from binary)

Data Analysis to Determine Success

- These outcomes will be readily transferrable via a set of tools and a best practices guide that will show how to improve firmware update security by incorporating these tools and following a workflow that will increase the integrity of firmware updates to the energy infrastructure in the future
- The criterion for success is that we can fully automate this procedure and can demonstrate successfully the identification of such a threat in a given firmware update

Technology Transition

- Project team will work closely with a selected DoD site to understand firmware installation/upgrade process and to demonstrate the value of incorporating of firmware analysis tools
- Boeing will evaluate commercialization opportunities as part of the proposed work in this proposal, alternatives include inclusion into base evaluation services
- LLNL, PNNL and Boeing have significant expertise in the commercialization of advanced technologies
- First potential users will likely be both base maintenance personnel, infrastructure security assessment teams and critical infrastructure vendors



Related Efforts

- DOE Office Of Electricity Delivery & Energy Reliability, Supply Chain Integration For Integrity (SCI-FI) project has funded the prototype firmware analysis tools
- DOE NNSA Stockpile Stewardship program investments apply ROSE to code verification and performance analysis
- DOE ASCR program investments apply ROSE to exascale computer architecture research
- IARPA investments in robustness of ROSE infrastructure
- Internal funding from DOE LLNL has supported general binary analysis capabilities in ROSE that are used as a basis for building firmware analysis tools

Expected DoD Benefits

- Benefits
  - Provide new capabilities to automate firmware analysis
  - Lower the cost of analyzing firmware, and quicker feedback
  - Enable building technician, untrained in cyber security, to identify suspicious software for further analysis
  - Integration into existing security assessments
  - Improve supply-chain integrity for mission-critical energy delivery systems and automated building control systems
- Answers to other questions
  - All DoD bases have a power distribution system and HVAC system, where they have embedded controllers (modern systems) there is firmware to be analyzed
  - The demo will communicate the rate of applicability of our technology to devices
  - We define an automated approach where only a manual approach exists today
  - Payback is dependent upon the costs of failure for critical infrastructure

Acknowledgments

Role	Institution	Name	Activities
PM	LLNL	Eddy Banks	Project manager to provide coordination of task execution, reporting and stakeholder interactions
Co-PI	LLNL	Dr. Markus Schordan	Lead program analysis work for analysis tools
Co-PI	LLNL	Ken Masica	Lead the engineering and security analysis of military base energy infrastructure systems and technologies
Co-PI	PNNL	Dr. David Manz	Lead evaluation on testbed facility at PNNL and tool packaging specifications
Co-PI	Boeing	Ryan Hammond	Lead connection to firmware analysis and operational use
Staff Programmer	LLNL	Robb Matzke	Support binary firmware analysis tools and robustness
Hardware Specialist	PNNL	Matt Engels	Support grid electronic devices used throughout the project
Staff Programmer	Boeing	Zach Thornton	Support binary firmware analysis tools

For additional information, please visit

https://www.serdp-estcp.org/Program-Areas/Energy-and-Water/Energy/Microgrids-and-Storage/EW-201608

Speaker Contact Information

dquinlan@llnl.gov; 925-423-2668

LLNL-PRES-704260
This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under contract DE-AC52-07NA27344. Lawrence Livermore National Security, LLC

Q&A Session 3

SERDP DOD • EPA • DOE | ESTCP

The next webinar is on October 20, 2016

"DoD Decision Making and Climate Change"

SERDP DOD • EPA • DOE | ESTCP

Survey Reminder

Please take a moment to complete the survey that will pop up on your screen when the webinar ends

SERDP DOD • EPA • DOE | ESTCP