The overall classification of this briefing is: UNCLASSIFIED//FOUO

Lead Sponsor: USCYBERCOM
Operational Endorsers: USPACOM, USSTRATCOM, OASD (AT&L)/EI&E, and NORAD-USNORTHCOM
J-BASICS GO Steering Council

- USCYBERCOM: Brig Gen Christopher Weggeman, Director J5
- DOT&E: Mr. Mike Crisp, Deputy Director, Air Warfare
- USNORTHCOM/NORAD: RDML Dwight Shepherd, Director J6
- USPACOM: Dr. George Ka’iliwai III, Director J8
- DISA/JFHQ-DODIN: Brig Gen Robert Skinner, Deputy Commander, JFHQ-DODIN
- National Guard: Maj Gen Kevin Bradley, National Guard Assistant to Commander USCYBERCOM and Director NSA
- OASD Energy, Installations and Environment/DASD IE: Ms. Lisa Jung
- USD(AT&L)/DASD(Emerging Capability & Prototyping): Mr. Earl Wyatt
Admiral Rogers at the Wall Street Journal WSJD Live Conference, 19 Oct 2015, Top Three Cyber Concerns:

#1. Cyber attacks that do infrastructure damage

"It is only a matter of 'when' that someone users cyber as a tool to do damage to the critical infrastructure of our nation," Rogers said.

"I'm watching nation states, groups within some of that infrastructure. At the moment, it seems to be really focused on reconnaissance and attempting to understand the characteristics of the structure, but it's only a matter of time I believe until someone actually does something destructive."
Response

“In addition, DOD has taken—or participated in—efforts to enhance department-wide cybersecurity of ICS. For instance, the United States Cyber Command and the Joint Test and Evaluation Program—under the Director, Operational Test and Evaluation, Office of the Secretary of Defense—initiated a collaborative effort in 2014 to develop a set of procedures to detect, mitigate, and respond to cyber incidents on DOD ICS perpetrated by advanced persistent threat actors, such as nation states. These procedures are intended to be employed by DOD installation personnel such as installation information technology managers and ICS facility engineers. An official from the command stated that the draft procedures will be tested at a joint exercise in June 2015 and expects the procedures to be completed by December 2015.” -- p. 35
Charter

FEB 26 2014

“employ multi-Service and other Department of Defense (DoD) agency support, personnel and equipment to develop, test, and evaluate advanced cyber industrial control system (ICS) tactics, techniques, and procedures (TTP) to improve the ability of ICS network managers to detect, mitigate, and recover from nation-state level cyber attacks”

Concept

Problem Statement

Network managers supporting DOD Industrial Control Systems (ICS) lack TTP to detect, mitigate, and recover from nation-state level cyber attacks.

Lead Sponsor

USCYBERCOM

Operational Endorsers

NORAD-NORTHCOM

OASD (AT&L)/EI&E

USPACOM

USSTRATCOM
Timeline

Phase I - Finalize Initial TTP & Prepare for FT-1
- Finalize Initial TTP Development
- Plan and Prepare for RRE and FT-1

- JWAG Review TTP
- Risk Reduction at NL

Phase II - TTP - Test and Refine
- FT-1 – Test Initial TTP
- Refine TTP

- JWAG Review TTP

Interim Product to Warfighter

Phase III - TTP - Test and Transition
- FT-2 – Test Refined TTP

Test and Transition
- Refine and Transition Final TTP to Warfighter
Tactics, Techniques & Procedures

Three Main Sections:
- Detect
- Mitigate
- Recover

Detailed Sections for:
- Baselining
- Routine Monitoring

Complements & Compatible with:
- CJCSM 6510.01B
- RMF
- NIST Standards
- CISA Ready
FT-1 to FT-2 Changes

TTP (Test Article)
• Mitigate TTP Updates
  – Provided more details for segmentation of varying network topologies
• Recovery TTP Updates
  – Added re-integration procedures to clarify the requirements for Operators
• Incorporated FMC baseline development information so that Operators could compare the baseline to observed system behavior
• Added section on Routine Monitoring to afford Operators an opportunity to conduct routine troubleshooting checks prior to cyber event checks

Test Event Design
• More focus on detect, especially w/o Adversary Present (false positives)
• Operational-style OPFOR
• Event streamlining
Field Test 2 Overview

• Location – Sandia National Labs (SNL)
• 2 Identical but separate ICS networks
• 1 Week of intensive training (1 – 5 June 2015)
• 2 Weeks of test events (8 – 19 June 2015)
• 4 Days during Cyber Guard 15
• Concurrent network and ICS technical training
• Air National Guard + SNL OPFOR
• 12 Participants from across the Services
  (6 Teams: 1 IT and 1 Facility Engineer)

- US Army Corp of Engineers
  - Tulsa, OK
  - Savannah, GA
  - Fort Huachuca, AZ
- US Naval Facilities
  - Southwest (San Diego, CA)
  - Southeast (Jacksonville, FL)
  - Mid-Atlantic (Norfolk, VA)
  - Marianas, Guam
- Joint Base Pearl Harbor-Hickam, HI
- Joint Base Elmendorf-Richardson, AK
- USMC, Marine Air-Ground Combat Command, 29 Palms, CA
- US Coast Guard
  - Command, Control, and Communications Engineering Center, Portsmouth, VA
  - Telecommunications and Information Systems Command, Alexandria, VA
Transition Actions

• Revise TTP for fielding
• Final Report
• Roadshow & Hand-over
  – Actions/Resource for Success & Sustainment
  – Organizations Visited
  – Exercises for FY16
TTP Success & Sustainment

1. Memo/TASKORD/Guidance to promulgate
   (USCYBERCOM/J3 lead, recommend tri-lateral guidance)
   - Use of the TTP in operations
   - Establish tasking/reporting channels & coordination
   - Establish base/post/camp-level responsibilities

2. Training
   - Materials for 2-5 day training including TTXs prepared (transition to USCYBERCOM/J7) – team of 2
   - Recommend SMEs be available to assist users in adapting TTP
   - Future options:
     • CBT, hands-on lab, local exercise integration
     • Persistent Training Environment ICS component

3. Maintenance/Outreach
   - Annual Refresh Cycle: PIT-CS Working Group to oversee
   - Configuration Manager/Editor/Publisher
   - Exercise engagement
   - SMEs
J-BASICS Outreach

• **Recent:**
  - FLEETCYBER/10th Fleet
  - MARFORCYBER
  - AFCYBER
  - JFHQ DODIN
  - USFK/PACOM
  - STRATCOM/Offutt
  - NORTHCOM/NORAD/Peterson
  - CENTCOM/SOUTHCOM/SOCOM
  - J-BASICS Joint Warfighter Advisory Group (includes Army COE, NAVFAC, AFCEC)
  - ICS-CERT (DHS) ICS Joint Working Group

• **Future:**
  - EUCOM/AFRICOM
  - TRANSCOM
  - Coast Guard/Alameda
  - Cyber Component Commanders’ Conference
  - Inside-the-Beltway briefings
J-BASICS Exercise Involvement (FY16)

- **PACIFIC SENTRY/GLOBAL LIGHTNING**
  - Joint PACOM/STRATCOM operational exercise
  - Exercise dates 23 – 29 APR 2016
  - J-BASICS TTP has been interwoven into the exercise scenario
  - PS/GL scenario directly plays into the Cyber Guard exercise scenario

- Cyber Guard Exercise
  - USCYBERCOM certification/capstone and tactical exercise
  - Exercise dates 10 – 18 JUN 2016
  - J-BASICS TTP has been interwoven into the exercise scenario
  - Working with our J3 and J7 counterparts to have J-BASICS TTP deployed with I&W for use by National Guard teams and potentially by their private sector partners
Action Items from GOSC #2

• Identify the broader community who should be aware of the J-BASICS TTP and engaged to institutionalize the TTP
  – PIT-CS WG in process of being established
    • Will oversee annual refresh cycle
  – Engaging all COCOMs and Cyber Component Commanders
  – Recognize opportunities for:
    • Private providers to DoD (via contractual agreements)
    • CIKR (via DHS)
    • State-level (via National Guard)
    • International (military partners and foreign private providers)

• Begin the process of identifying the priorities against which to deploy the J-BASICS TTP. This needs to include understanding the connected dependencies
  – Recommended Priorities:
    • Defense Critical Infrastructure
    • Other DoD-owned Infrastructure
    • DoD Privatized
  – Observation: “Ultimately, everything appears to be interconnected now”
GO/FO Awareness & Engagement

• #1 Question from the field: “How is this being resourced?”
  – Messaging: Not a new requirement, rather helps to streamline actions needed to meet existing requirements
  – More resources are needed with the ICS community to adequately cover existing cyber requirements
  – Continue to resource annual update/exercise/promulgation (USCYBERCOM, AT&L)

• Clarify roles WRT J-BASICS TTP ownership & processes
  – USCYBERCOM, OASD (EI&E), JFHQ-DoDIN
  – TASKORD/Memo/Guidance to operationalize

• Drive incorporation of “ICS Thinking” into mission
  – In planning
  – In exercises
  – Among personnel across the department – make it a part of “cyber culture”

Get the word out: ICS Operators may well be on the frontlines at the start of the next fight. Prepare Now!
DISCUSSION
Backup
## Warfighter Established Criteria

<table>
<thead>
<tr>
<th>Measure</th>
<th>WEC</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FT-1</td>
<td>FT-2</td>
<td></td>
</tr>
<tr>
<td><strong>Issue 1 (Detect):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% detect adversary present (sensitivity)</td>
<td>40%</td>
<td>60%</td>
<td></td>
</tr>
<tr>
<td>% no detect/no adversary present (specificity)</td>
<td>70%</td>
<td>70%</td>
<td></td>
</tr>
<tr>
<td><strong>Issue 2 (Mitigate):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% effective mitigations</td>
<td>70%</td>
<td>80%</td>
<td></td>
</tr>
<tr>
<td><strong>Issue 3 (Recover):</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% Recovery to fully mission capable state</td>
<td>60%</td>
<td>60%</td>
<td></td>
</tr>
</tbody>
</table>

WEC values established at J-BASICS JWAG April 2014 and revalidated at J-BASICS JWAG March 2015
## FT-2 Test Accomplishments

<table>
<thead>
<tr>
<th></th>
<th>Planned</th>
<th>Conducted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required # of FT-2 Events</td>
<td>FT-2 Events</td>
</tr>
<tr>
<td>Detect (AP)</td>
<td>23</td>
<td>23</td>
</tr>
<tr>
<td>Detect (NAP)</td>
<td>22</td>
<td>23</td>
</tr>
<tr>
<td>Mitigate</td>
<td>36</td>
<td>41</td>
</tr>
<tr>
<td>Recover</td>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>95</td>
<td>102</td>
</tr>
</tbody>
</table>

FT-2: Field Test 2  
CG: Cyber Guard  
AP: Adversary Present  
NAP: No Adversary Present  
FP: Free Play
Overall Results

• Detect:
  – TTP allowed Operators to detect as designed. TTP was designed to:
    • Reject false positives (high specificity)
    • Mid-level detect rate (lower than 75% sensitivity)
  – TTP allows for an approximate 10-time increase in the odds of detecting an adversary if the adversary is present
  – Results show that the more information provided to the user, the more successful the operator will be in using the TTP to detect an adversary

• Mitigate: Results show that the more complex the mitigate task, the harder the mitigation becomes

• Recover: TTP was successful in enabling Operators to restore devices to FMC and reintegrate those devices back into network
FT-2 to TTP Fielding Revisions

- **Concepts**
  - Added chart depicting the flow from detection to mitigation and then to recovery.

Chart 1: Detection, Mitigation, and Recovery Overview
**Revised the Event Diagnostic Table**

### ENCLOSED A: DETECTION PROCEDURES

#### A.1 Event Diagnostics

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Notification</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.1 Notifications</td>
<td>Cyber event notifications are issued by a variety of entities. These include: UCSCYBERCOM, ICS-CERT, or the Department's directives.</td>
<td>A-5</td>
</tr>
</tbody>
</table>

**Server/Workstation Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.2 Log File Check: Unusual Account Usage/Activity</td>
<td>Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in 2. Rapid and/or continuous log-ins/ log-outs 3. Users logging into accounts outside of normal working hours 4. Numerous failed log in attempts 5. User accounts being granted to escalate account privileges.</td>
<td>A-7</td>
<td></td>
</tr>
</tbody>
</table>

**Network Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Notification</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.9 Network Anomalies: IDS Exhbiting Unusual Behavior</td>
<td>A-10</td>
<td></td>
</tr>
<tr>
<td>A.2.10 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred</td>
<td>A-11</td>
<td></td>
</tr>
<tr>
<td>A.2.11 Network Anomalies: Firewall Exhibiting Unusual Behavior</td>
<td>A-12</td>
<td></td>
</tr>
</tbody>
</table>

**Server & Workstation Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.22 Field Device: Abnormal decrease in Control Process Traffic</td>
<td>Any host, including SCADA equipment: 1. Spontaneous reboot or screen saver change 2. Unusually slow performance or usually active CPU 3. CPU cycles up and cycles down for no apparent reason 4. Intermittent loss of mouse or keyboard 5. Configuration files changed without user or system administrator action in operating system 6. Configuration changes to software made without user or system administrator action 7. System unresponsive</td>
<td>A-13</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.23 Field Device: Unexpected changes to: Ladder Logic/Code Configurations</td>
<td>A-24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.24 Field Device: HMI/OPC/Control Server sending false information</td>
<td>A-25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.25 Field Device: HMI/OPC/Control Server sending false information</td>
<td>A-26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.26 Field Device: Malware</td>
<td>A-27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.27 Field Device: Unusual Field Device Activity Observed/Reported</td>
<td>A-28</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### ENCLOSED A: DETECTION PROCEDURES

#### A.1 Event Diagnostics

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.1 Notifications</td>
<td>Cyber event notifications are issued by a variety of entities. These include: UCSCYBERCOM, ICS-CERT, or the Department's directives.</td>
<td>A-5</td>
<td></td>
</tr>
</tbody>
</table>

**Server/Workstation Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.2 Log File Check: Unusual Account Usage/Activity</td>
<td>Any host server or workstation, including SCADA equipment. Anomalous entries can include: 1. Unauthorized user logging in 2. Rapid and/or continuous log-ins/ log-outs 3. Users logging into accounts outside of normal working hours 4. Numerous failed log in attempts 5. User accounts being granted to escalate account privileges.</td>
<td>A-7</td>
<td></td>
</tr>
</tbody>
</table>

**Network Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Notification</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.9 Network Anomalies: IDS Exhbiting Unusual Behavior</td>
<td>A-10</td>
<td></td>
</tr>
<tr>
<td>A.2.10 Network Anomalies: Firewall Log Indicates Anomalous Event Occurred</td>
<td>A-11</td>
<td></td>
</tr>
<tr>
<td>A.2.11 Network Anomalies: Firewall Exhibiting Unusual Behavior</td>
<td>A-12</td>
<td></td>
</tr>
</tbody>
</table>

**Server & Workstation Anomalies**

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.22 Field Device: Abnormal decrease in Control Process Traffic</td>
<td>Any host, including SCADA equipment: 1. Spontaneous reboot or screen saver change 2. Unusually slow performance or usually active CPU 3. CPU cycles up and cycles down for no apparent reason 4. Intermittent loss of mouse or keyboard 5. Configuration files changed without user or system administrator action in operating system 6. Configuration changes to software made without user or system administrator action 7. System unresponsive</td>
<td>A-13</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section Event</th>
<th>Event</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.23 Field Device: Unexpected changes to: Ladder Logic/Code Configurations</td>
<td>A-24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.24 Field Device: HMI/OPC/Control Server sending false information</td>
<td>A-25</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.25 Field Device: HMI/OPC/Control Server sending false information</td>
<td>A-26</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.26 Field Device: Malware</td>
<td>A-27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A.2.27 Field Device: Unusual Field Device Activity Observed/Reported</td>
<td>A-28</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>