## Recent Cyber-Scary Headlines

<table>
<thead>
<tr>
<th>Title</th>
<th>Author/Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Year in Cybersecurity: 5 Threats to Watch in 2015</td>
<td>By Julianne Pepitone, NBC News, Tuesday, 30 Dec 2014</td>
</tr>
<tr>
<td>The scary state of cybersecurity</td>
<td>By Kevin G. Coleman, C4ISR &amp; NETWORKS, August 14, 2014</td>
</tr>
<tr>
<td>Hackers Remotely Kill a Jeep on the Highway—With Me in It</td>
<td>By Andy Greenberg, C4ISR &amp; NETWORKS</td>
</tr>
<tr>
<td>5 charts that show cyber threats are growing</td>
<td>By Priya Anand, MarketWatch, Published: Oct 15, 2015 10:35 a.m. ET</td>
</tr>
<tr>
<td>This terrifying chart explains why cybersecurity is such a big problem for the government</td>
<td>By Andrea Peterson, The Washington Post, June 18, 2015</td>
</tr>
<tr>
<td>Hacking For Cause: Today’s Growing Cyber Security Trend</td>
<td>By Dan Lohrman, Crunch Network</td>
</tr>
</tbody>
</table>
Objective of Today’s Events

• Open a dialogue with industry on the unique cybersecurity requirements and challenges faced by the NAVSEA Enterprise

• Introduce the cybersecurity community to the NAVSEA Enterprise

• Answer industry questions on NAVSEA’s cybersecurity vision for the near and mid-term
Topics

• NAVSEA Enterprise Overview
• Cybersecurity Design Drivers
• CIO Responsibilities and Challenges
NAVSEA at a Glance

- People: 70,000+
- Locations: 30+
- Total acquisition programs: 150
- Budget: $30+ billion
- Total information systems: 1800+
We Build Ships and Ship Systems
We Design and Deliver

• Combat Systems
• Hull, Mechanical, and Electrical Systems
• Interior Communications
• Navigation Systems
Types of Systems

1. Defense Business Systems (DBS)
2. Navy Control Systems (Afloat and Ashore)
3. Research, Development, Test, and Evaluation Systems
4. Maintenance Systems
5. Test and Range Control Systems
6. Training Systems

It’s all about the ships!
System Design through the 1990s: Mission Focused

• Government-off-the-shelf (GOTS)
  – MILSPEC’d OSs, computers, message formats and protocols
  – Point-to-point analog and serial hardwire connections
  – Segregated, secure communications via TYPE I encrypted TADILs

• Security attributes of….
  – Confidentiality
  – Availability
  – Integrity

  …. were assured by system design

• Migration to commercial-of-the-shelf (COTS) technology introduced unexpected challenges, to include cyber security issues

Must Balance Mission and Security
Four Principle Tenets:

- Detect
- Protect
- React
- Recover

Requires complementary cybersecurity solutions across networks to create a seamless cybersecurity architecture.
Cybersecurity Key System Attributes

- Resiliency: Fights through cyber attacks
- High degree of automation
- Complementary cybersecurity solutions across independent and integrated security architectures
- Network growth without compromising security
- Cyber situational awareness
- Boundary defense capabilities at network control points
CIO Responsibilities

Enterprise Lead:
– NAVSEA Cyber Security Strategy
– Enterprise-wide IT/IS and Cybersecurity policy and guidance
– Enterprise Network Operations and Cyber Incident and Response
– Cybersecurity Risk Management Framework for DBS and Shore Infrastructure
– Cyber Audits, Inspections, and Technical Assist visits
– IT/IS and Cyber Competency, Workforce Development, and Training
– Information Management
– NAVSEA IT/IS compliance with the Americans with Disabilities Act (ADA)

Headquarters:
– IT/IS Service Delivery for 3500+ Personnel
Unique Challenges

• Implementation of Enterprise Cybersecurity Strategy

• Protection of Unclassified, Critical Technical Information on cleared defense contractor networks and systems

• Cyber workforce development and training
Enterprise Cybersecurity Strategy

• Today, many commands and field activities have implemented the required protective measures

• Require a common Enterprise solution for....
  – Continuous monitoring
  – Situation awareness
  – Cyber incident and response
  – Command and control across the various commands

• Developing a Test Bed to complete technical evaluations of new technologies
Unclassified Critical Technical Information

- DFAR 252.204-7012: “Safeguarding Covered Defense Information and Cyber Incident Reporting”

- Initial discussion held with shipbuilders
  - What constitutes “Unclassified Critical Technical Information”?
  - How does a prime flow down the requirements to Sub-contractors?
  - What requirements should CDCs IS’s meet? (NIST SP 800-171)
  - How do we address information that’s been in the public domain for several decades?
  - At what cost?
# Proposed Cyber Security Training Construct

<table>
<thead>
<tr>
<th>Training Series</th>
<th>Target Audience</th>
<th>Shore Billets / Job Series / NEC¹</th>
<th>Ship Billets / NEC²</th>
<th>Delta Knowledge, Skills, Abilities (KSA) from Job Series or NEC</th>
<th>Course Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 CYBER AWARE</td>
<td>ALL IS Users</td>
<td>All</td>
<td>All</td>
<td>N/A</td>
<td>101</td>
<td>DAU CLE 074 - Cyber Security Throughout DoD Acquisition</td>
</tr>
<tr>
<td>200 CYBER SMART</td>
<td>Decision Makers</td>
<td>Ex: PEO/ED/TD/MPM/DPM</td>
<td>CO/XO/DH</td>
<td>N/A</td>
<td>201</td>
<td>USNA Course Si110</td>
</tr>
<tr>
<td>300 CYBER ADVANCED ENGINEERS</td>
<td>Ex: 0801, 0854, 1550</td>
<td>Ex: EMO, STO, C5I Officer, SIWO, FC, ST, ET, IC</td>
<td>Example: Software Engineer</td>
<td>Ability to Lock Down OS 301 Secure Coding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>400 CYBER EXPERT</td>
<td>Cyber Engineers</td>
<td>Ex: 2210</td>
<td>Ex: 2201, 2791 SYSAADMIN</td>
<td>Ability to Lock Down OS 301 Secure Coding</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NAVSEA is in need of cybersecurity courseware and technical services support in a number of areas
We Have....
COTS and GOTS,
COTS ON GOTS,
GOTS ON COTS,
BOTS on COTS,
BOTS on GOTS,
BOTS ON COTS ON GOTS
AND LOTS AND LOTS AND LOTS OF BOTS!

THIS ISN’T CHILD’S PLAY...

WE NEED YOUR HELP!

All images taken from www.seusville.com
• BACKUP SLIDES
Test and Range Facilities
NAVSEA Builds or Maintains 90+ Trainers in 16 Site locations

*VETT and MMTT support multiple courses of instruction