



Joint Information Environment (JIE) & Coast Guard

Rear Admiral Bob Day, CG CIO & Director CG Cyber
Command

22 May 2013
*AFCEA-GMU C4I
Center Symposium*



Homeland
Security

JIE

- J= Jolly
- I= Interesting
- E= Endeavor

Especially for U.S. Coast Guard!!!

JIE

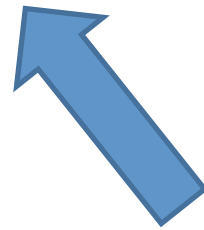
- J= Jeopardy
- I= If
- E= Evaded

For All!!!

JIE



HSIE



Pick a team.....but I have to be on both to do my job!!!!

All Sorts of Opinions

We are getting  Google[™]

We are getting  Scroogled

RADM Day's Opinion

- This just the next, and correct, evolution of IT infrastructure and services.
- JIE lays the needed framework to:
 - Drive much needed configuration and standards.
 - Significant enhances security and the ability to defend our critical networks and assets.
 - Enhances full interoperability and joint training.
 - Facilitates implementation of mobility and big data.
 - And “can” provide much needed efficiencies to “hopefully” reinvest in new capabilities.

RADM Day's Opinion

“JIE and HSIE is going to help me solve some of my most pressing C4IT problems by establishing enterprise wide mandates that programs cannot ignore”

What's Problems?

- **Resources are going to continue to shrink.**

We cannot afford the programs we have and the way we currently manage IT.

- **Configuration Management.**

Poor processes and adhoc compliance at all levels result in inefficiencies and significant security weaknesses.

- **Command & Control.**

Current processes have too many layers and as a result are too slow to meet performance mandated by US Cyber.

- **Workforce Skills.**

We are not responding to the change signal for the work force skills and competencies needed in current/future environment.

\$'s for FY13-XX

- **C4IT Budget:**

FY10 \$436M FY11 \$476M FY12 \$483M

FY 13 (projected) \$486M

The numbers are deceiving. For example, FY13 includes \$16M for St. Elizabeth's move, support \$'s for new assets coming online (FRC, NSC, R21 maintenance). Reality is that we have lost over \$53M in budget during FY11-12 (efficiency mandates) have required significant cuts to some services and elimination of many new initiatives. FY14-15 projections are downright scary.

- **20% HQ personnel reductions have really hurt capacity.**

- **C4ITSC and Field reductions slated for FY14/15.**

Configuration Management

- **The negative impacts of our current state (poor) have been fully demonstrated by several recent events.**
 - **Misconfigured personal folders. Almost 4 months since identified and we still have not fixed. C4IT budget at risk for \$300K as a results of privacy concerns.**
 - **Wireless routers and prohibited devices routinely found connected to CG One. Time to ID and remediate these serious security risks is unacceptable.**
 - **Applications and systems installed with no ATO or security packages routinely identified.**

Configuration Management

- **Our processes for proposing, developing, and implementing changes need improvement and when fixed, must be followed by all.**

- **Distribution Group script debacle is a perfect example of the havoc that can result as well as the significant overall cost and potential mission impact to the CG.**
- **1000's of man-hours are spent remediating errors that should have never occurred if proper CM was followed. Open personal folder issue, vulnerability remediation, and constant re-imaging of workstations because of security issues waste our workforces time.**

Configuration Management

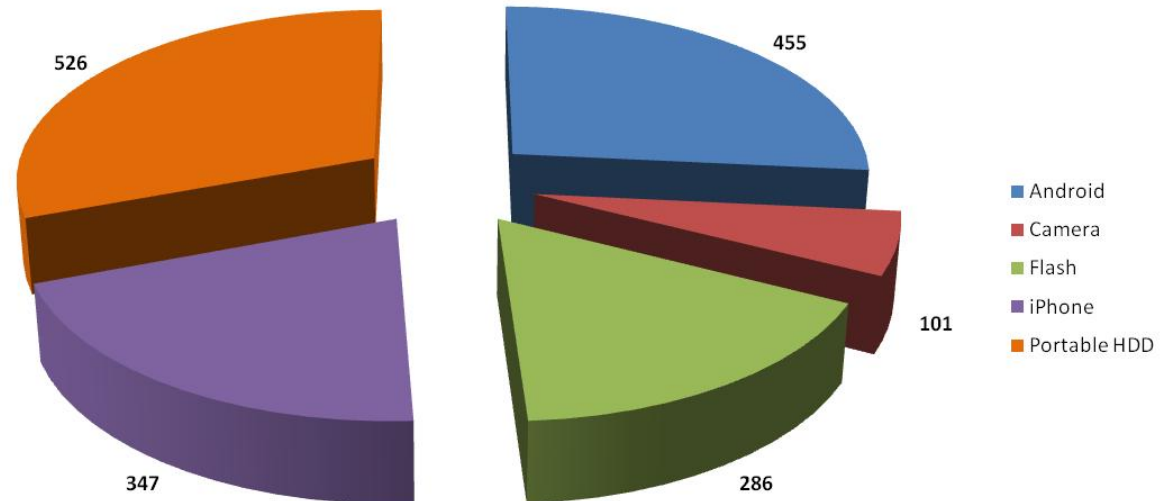
- **Lack of user and administrator accountability for poor security and CM performance is contributing to the overall problem.**
 - OPSEC violations especially user names and passwords.
 - USB devices.
 - Rogue software including executables.
 - Unaccredited systems.
 - Lapsed ATO's.
 - Failure to use mandatory procurement sources.
 - "Reply All" use during last weeks DG event.

We must put some tooth into CM/Security programs!

High Risk Device Usage

| Month | Android | Camera | Flash | iPhone | Unencrypted HDD | Total |
|------------|---------|--------|-------|--------|-----------------|--------|
| Oct - 2012 | 281 | 89 | 424 | 190 | 14,334 | 15,318 |
| Nov - 2012 | 304 | 64 | 280 | 397 | 4,678 | 5,723 |
| Dec - 2012 | 250 | 60 | 175 | 279 | 1,729 | 2,493 |
| Jan - 2013 | 455 | 101 | 286 | 347 | 526 | 1,715 |

High Risk Device Usage



Command & Control

- **The nature of the Cyber threat, expectations of US Cyber, and the criticality of our IT systems to mission execution requires C2 that:**
 - Has real time situational awareness.
 - Is guided by doctrine and standardized TTP.
 - Has a single point for contact and reporting.
 - Is recognized by all as the authoritative entity.
 - Works at near machine speed.

Our current IT management structure and processes do meet these C2 requirements.

Workforce

- **Consolidation, Virtualization, As A Service, and budget will require significant shifts in the organization, skills, and duties of our IT workforce.**
- **New emphasis include cyber security processes, managing and leveraging “big data”.**
- **As systems collapse so will the workforce. The days of being a “server hugger” are almost over.**

So what are we doing?

- **The budget and oversight environment is going to force the following:**

- Consolidation of like requirements into single programs of record and termination of legacy/program specific systems.
- Centralization of IT budgets and procurement.
- Use of Agency wide services like Defense Enterprise E-mail even if more expensive than current systems.
- Mandatory use of Agency centralized procurement vehicles.
- Pervasive oversight and reporting.

This will significant changes in our current processes and overall organizational structure.

So what are we doing?

- **Implement and maintain ruthless configuration management to include the following:**

- Establish new levels of segregation of administrator permissions and authorities. Strict qualification standards and oversight for enterprise level and complex functions.
- New paradigms for change requests, development, and implementation.
- Mandatory compliance. Short term waivers provided for only the most urgent operational needs after centralized risk based review is conducted.
- Mandatory use of security appliances (HBSS etc.).

This will be a significant culture change!!!!

So what are we doing?

- **Revamp Command & Control:**
 - Centralize tactical command and control by collapsing multiple operational watches and extracting C2 functions from product lines.
 - De-layer current C2 to create a single point for situational awareness, reporting (both up and down), and authoritative tasking.
 - Operationalize C2 with standard procedures (QRC's) mirrored on C2 processes from US Cyber/Fleet Cyber Command.
 - 24x7x365 organization focused on assessing the operation of the enterprise, generating required responses in minutes.

So what are we doing?

- **Design and build the future workforce:**
 - **Emulate Navy Information Dominance framework and competencies. Blending of IT, Intel, and Operations skills.**
 - **Leverage DoD schools where possible.**
 - **New career paths and likely new assignment and retention policies because of the significant training investment.**

RADM Day's Opinion

“These are not technology challenges, they are cultural and will require revamped business processes. Thus, it will be very challenging”.

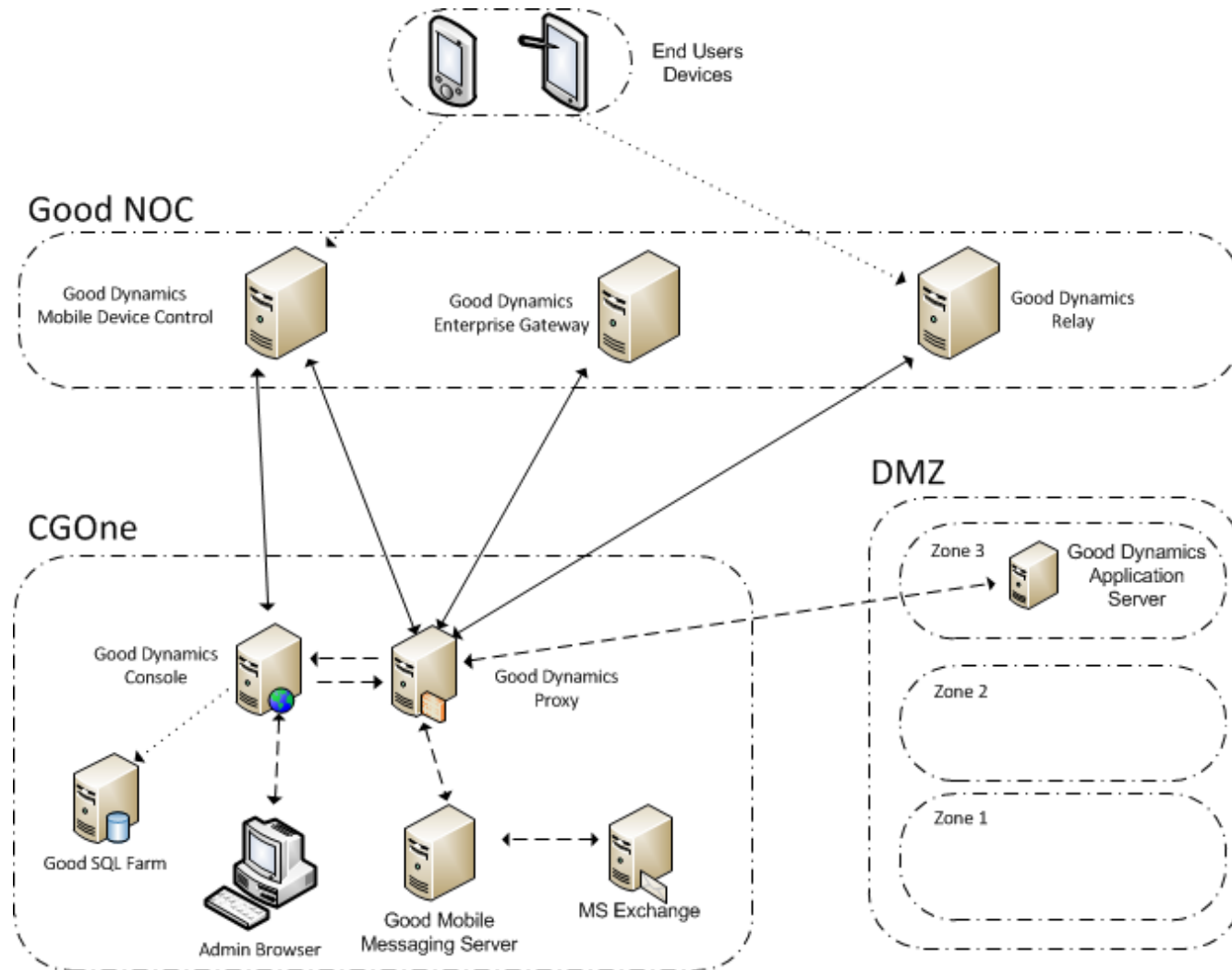
Mobility



Leveraging Others

- Leveraging DOD progress
 - Working with DOD as DISA creates iOS5 STIG
 - DOD/DISA application store
 - Secure provisioning and distribution of “vetted” applications
 - DISA - Smartphone training for users
 - DISA – Set up Internet Proxy
- DOD initiatives and successes
 - iOS5 STIG gaining traction
 - DOD implementing pilots similar to our Wireless Email
- Apple iOS moving along in the FIPS certification

CG Mobility Network Infrastructure



CG Electronic Flight Bag Initiative

The image displays a screenshot of an iPad's App Store interface. On the left, several callout boxes with arrows point to specific applications in a list. The applications listed are:

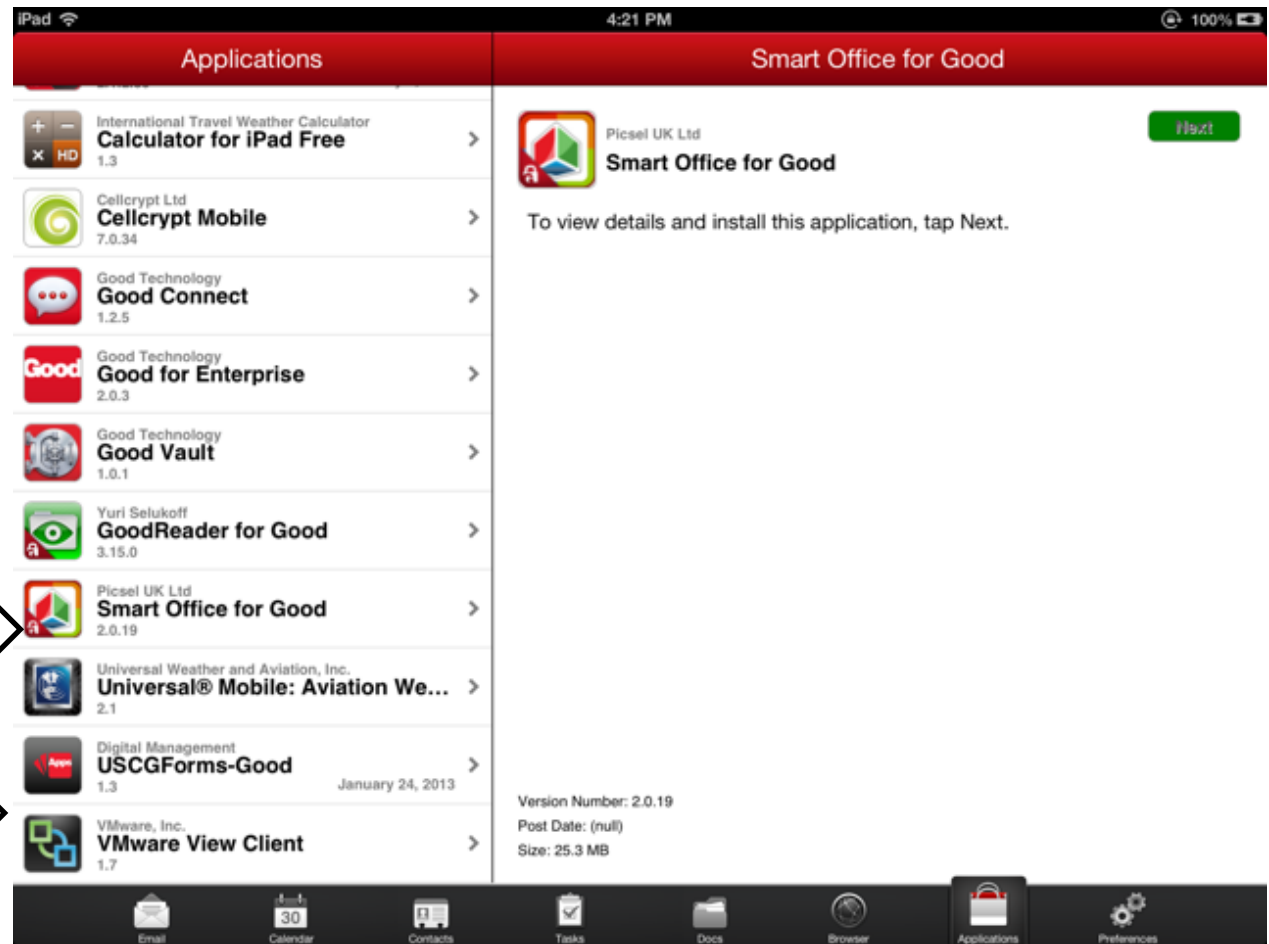
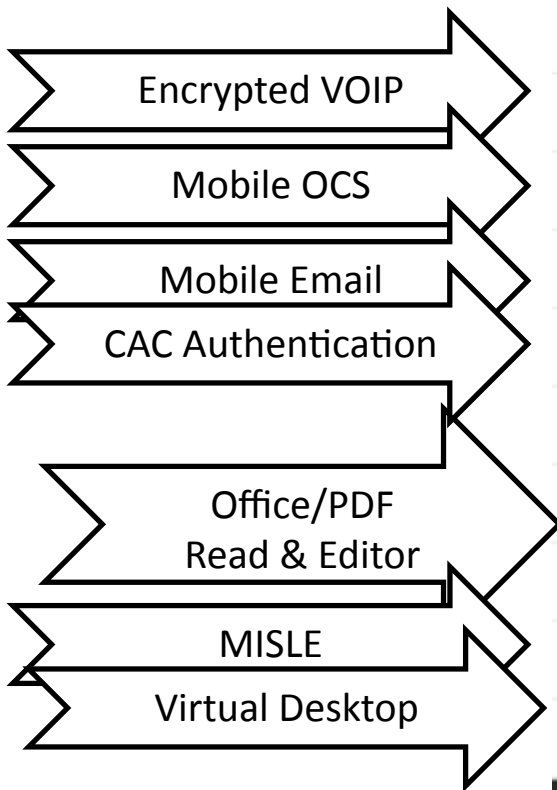
- Bad Elf GPS (2.0.14)
- International Travel Weather Calculator Calculator for iPad Free (1.3)
- ForeFlight Mobile (4.7.3)
- Good for Enterprise (2.0.3)
- GoodReader for Good (3.15.0)
- Jeppesen Mobile FD (v 2.0)
- PilotFAR / AIM (5.2.7)
- Smart Office for Good (2.0.19)
- Universal Mobile: Aviation We... (2.1)
- WSI Pilotbrief Optima Enterprise (1.4.1)

On the right side of the screen, the details for the 'AccellionGD' app are shown, including an 'Install' button. Below the app list, the following information is visible:

- Version Number: 2.1.2.30
- Post Date: January 9, 2013
- Size: 12.3 MB

The iPad's home screen dock is visible at the bottom, containing icons for Email, Calendar, Contacts, Tasks, Docs, Browser, Applications, and Preferences. The top status bar shows the time as 3:40 PM and 100% battery.

Future CG Mobility



The CG Mobile App

“Public Facing”

- Direct Public Outreach
- Access to CG resources where people use them most.
- Available for free via Android and IOS App Stores.
- Leverages the power of smartphone technologies.



Proposed Initial Use Cases

1. “Call the Coast Guard” Button

- Dials one of the 35 CG Sectors based on the phone’s current location.
- Gives advice on how and when to report certain incidents / displays lat/lon during the call.
(Warning Disclaimer regarding cell-coverage and use of CH-16)

2. Fill out a FLOAT PLAN

- Option to email the plan to a responsible party
- Instructions on how to use a float plan effectively

3. Submit an “NRC Report” (Oil Spill / Security Incident / Other)

- Optional “Dial the NRC” button
- Emails NRC Report contents along with present location.

4. Submit a location-based ATON Discrepancy Report to the Nearest CG Sector

- Emails location and optional picture of the aid (Non Real-time disclaimer)

5. Request a Vessel Inspection (from the CG Auxiliary)

- Emails form data to the Aux.

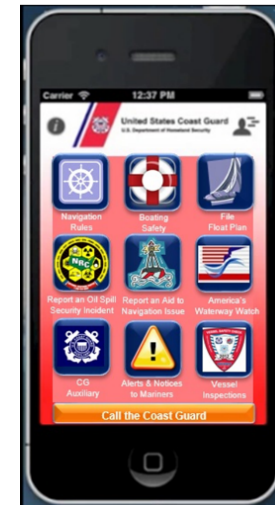
6. Alerts & Notices to Mariners

- Pulls information as a news feed based on the phones current location.

7. Boating Safety Tips, News & Information

8. Navigation Rules & Information

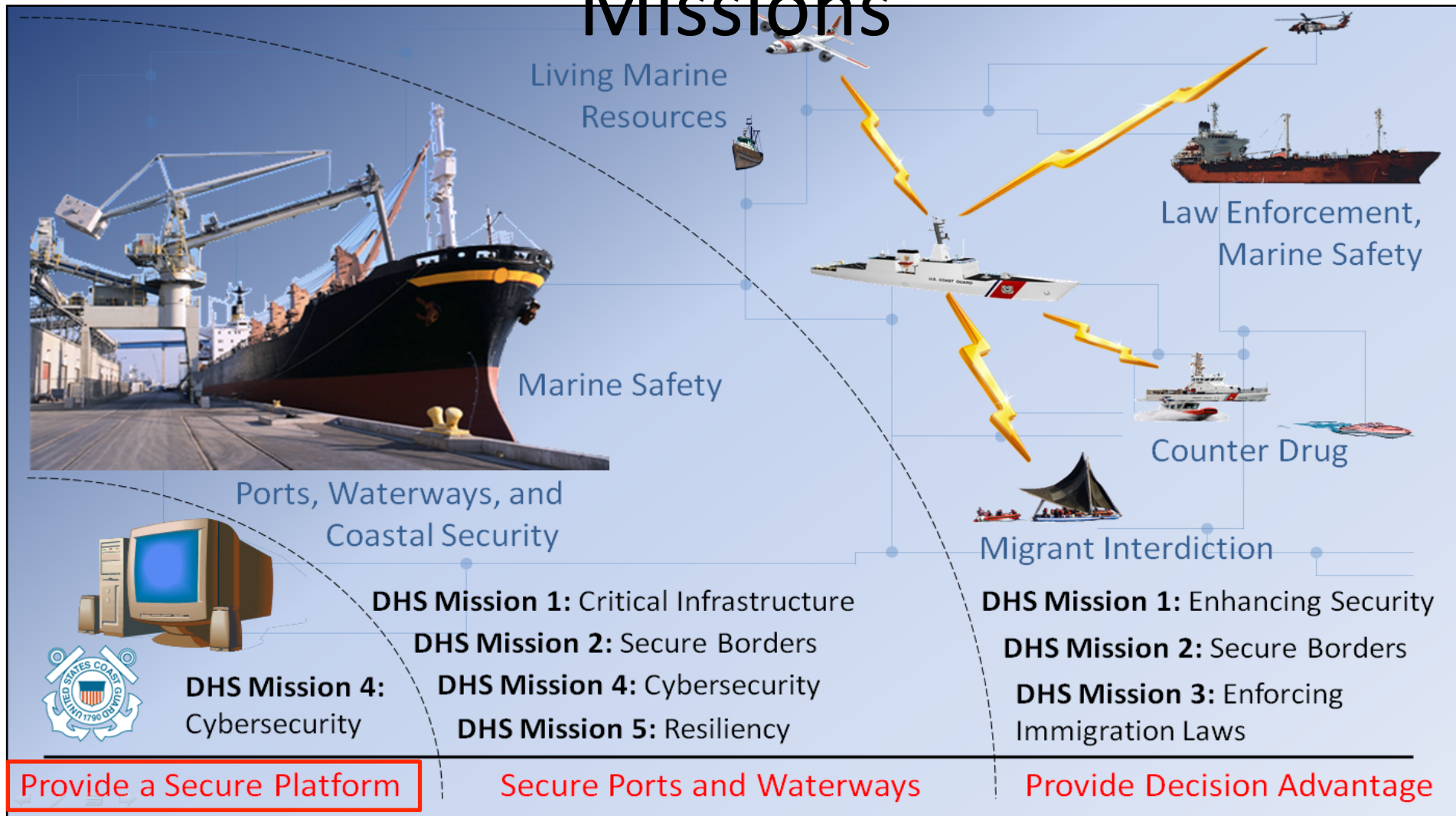
9. America’s Waterways Watch



Cyber



Missions



Computer Network Defense

(CND)

- CSOC operating at TS//SCI level.
 - Real time comms w/ key cyber centers
 - USCYBERCOM (.mil)
 - DHS SOC (.gov)
 - National Cybersecurity & Communication Integration Center (NCCIC) (MCIKR)
- CSOC Sensors
 - DOD Trusted Internet Connections
 - MALWARE Host Based Security Services (HBSS)
 - Upgraded Intrusion Detection Systems
 - Data Loss Prevention (DLP) System used for OPSEC

SHODAN

Internet Control System Indexing Site

Risk to Maritime CIKR

&

USCG Non-Standard Systems

SHODAN - Computer Search Engine - Windows Internet Explorer provided by U. S. Coast Guard UNCLASSIFIED

http://www.shodanhq.com/home

File Edit View Favorites Tools Help

http://intelreport.mandi... SHODAN - Computer Se... SHODAN - Computer ... x :// Free online network tool... Default Passwords | CIR... Home Feeds (1) Print Page Tools

Main Exploits Research Videos Anniversary Promotion Settings Logout Buy

SHODAN USCG Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

Dashboard History

Dashboard

Recently Shared Search Queries

| | |
|--|---|
| no... alt | 1 |
| http://www.shodanhq.com/host/view/93.172.169.182 | 1 |
| ist | 1 |
| cisco | 2 |
| real.de | 2 |

» See more recently shared searches

Popular Shared Search Queries

| | |
|------------------|-----|
| Webcam | 633 |
| Netcam | 207 |
| dreambox | 161 |
| default password | 137 |
| netgear | 116 |

» See more popular, shared searches

Your Recent Searches


Note: Click here to enable the search history feature.

Quick Filter Guide

| | |
|----------------------|--|
| after/ before | limit results by date in the format day/month/year (ex. before:20/03/2010) |
| city | name of the city (ex. city:"San Diego") |
| country | 2-letter country code (ex. country:US) |
| geo | latitude and longitude (ex. geo:50.23,20.06) |
| port | 21, 22, 23, 80, 161 or 443 |
| os | operating system (ex. os:Linux) |
| net | IP range using CIDR notation (ex. net:18.7.7.0/24) |
| hostname | full or partial host name (ex. hostname:google) |

» Complete filters reference

0 Credits

 CONTACT ME STAY UP TO DATE FOLLOW ME ON TWITTER

For direct inquiries: jmath@shodanhq.com

Add-Ons

Note: Click here to learn about available add-ons.

API Key

Note: You haven't yet created an API key. Click here to create an API key for your account.

Sponsor

Find SQL Injections, XSS problems in your website for free

Hurricane LABS

Internet | Protected Mode: On 100%

SHODAN - Computer Search Engine - Windows Internet Explorer provided by U. S. Coast Guard UNCLASSIFIED

http://www.shodanhq.com/search?q=uscg

File Edit View Favorites Tools Help

http://intelreport.mand... SHODAN - Computer Se... SHODAN - Computer ... x :// Free online network tool... Default Passwords | CIR... Home Feeds (1) Print Page Tools

Keep-Alive: timeout=60, max=2000
Location: http://189.137.203.182/login.lp
Set-Cookie: xAuth_SESSION_ID=1zC3805XINmrsu1USCG4JgA=; path=/
Cache-control: no-cache="set-cookie"

Google
74.125.31.66
Google
Added on 07.04.2013
Mountain View
Details
tb-in-f66.1e100.net

HTTP/1.0 200 OK
Date: Sun, 07 Apr 2013 09:41:04 GMT
Expires: -1
Cache-Control: private, max-age=0
Content-Type: text/html; charset=ISO-8859-1
Set-Cookie: NID=67=u008BkEM-Ew42M0zrzrWa7viDNQ_dqoph547jEJGUQse-boe92dlWafQUWqghXybxkfP6zLEb7CIj4YdvglUSCGS16oRC115JK7JK0hIHkHRZDkCQqCJk804Mes3XoWk; expires=Mon, 07-Oct-2013 09:41:04 GMT; path=;/ domain=.; HttpOnly
P3P: CP="This is not a P3P policy! See http://www.google.com/support/accounts/bin/answer.py?hl=en&answer=151657 for more info."
Serve...

216.92.6.200
pair Networks
Added on 07.04.2013
Pittsburgh
Details

HTTP/1.0 302 Found
Date: Sun, 07 Apr 2013 07:59:15 GMT
Server: Apache/2.2.24
Location: http://a05313.uscgaux.info/USCG_Aux_Info.php
Content-Length: 0
Content-Type: text/html

173.245.38.113
Kira Inc USCG
Added on 05.04.2013
Van Nuys
Details

Linux Kira_Inc_USCG 2.4.31-uo0 #1 Tue Jul 27 00:32:37 PDT 2010 armv5b

Error 401
72.215.154.204
Cox Communications
Added on 05.04.2013
Norfolk
Details

HTTP/1.0 401 Unauthorized
Connection: Keep-Alive
Cache-Control: no-cache
WWW-Authenticate: Digest realm="USCG 4TH FL CONF RM", domain="/", nonce="1073adf490b", algorithm="MD5", qop="auth"
WWW-Authenticate: Basic realm="USCG 4TH FL CONF RM"
Content-Type: text/html
Content-Length: 290

1 2 3 next >

Internet | Protected Mode: On 100%

Host Profile: 72.215.154.204

IP: **Summary**
Location: Norfolk, United States
Latitude/ Longitude: 36.8468, -76.2852

HTTP

HTTP/1.0 401 Unauthorized
Connection: Keep-Alive
Cache-Control: no-cache
WWW-Authenticate: Digest realm="USCG 4TH FL CONF RM", domain="/", nonce="1073adf480b", algorithm="MD5", qop="auth"
WWW-Authenticate: Basic realm="USCG 4TH FL CONF RM"
Content-Type: text/html
Content-Length: 290

HTTP

HTTP/1.0 401 Unauthorized
Connection: Keep-Alive
Cache-Control: no-cache
WWW-Authenticate: Digest realm="USCG 4TH FL CONF RM", domain="/", nonce="1073adf464f", algorithm="MD5", qop="auth"
WWW-Authenticate: Basic realm="USCG 4TH FL CONF RM"
Content-Type: text/html
Content-Length: 290

SNMP

TANDBERG Codec
SoftW: F9.1.2 NTSC
MCU: TANDBERG Edge 95MXP
Date: 2012-01-10
S/N: 26B19170
BootSW: Rev. 1.16, 2009-01-21
Board: 101070 rev. 07

Search About 58,600 results

Web

Default Passwords | CIRT.net www.cirt.net/passwords?vendor=Tandberg - Cached 5. Tandberg - Video Communication Server. Version, 5.0. Method, ssh. User ID, root. Password, TANDBERG. Level, administrator ...

Images

Videos

News

TANDBERG IP Password - Video conferencing / Telepresence Forum www.vtctalk.com/forum/showthread.php?t=25449 - Cached command: ippassword <ip-password>. The default IP username and password is "TANDBERG". To remove this password, use the command: ...

Shopping

More

Show search tools

Tandberg default passwords www.default-password.info/tandberg/ - Cached - Similar DefaultPassword. + Help us, add your devices! Home Tandberg. Tandberg devices. 6000MXP, 1 password. TANDBERG - 8000, 1 password. © Analogic s.r.o. ...

TANDBERG VCS - Videoconferencia www.videoconferencia.es/.../TANDBERG_VCS_GettingStarted_Guide_en.pdf - Cached tandberg login: Enter the username. 6. admin and press Enter. You will get the password prompt: Password: Enter the default password of. 7. TANDBERG and ...

Default Credentials for Root Account on Tandberg E, EX and C ... www.cisco.com/en/US/products/.../cisco-sa-20110202-tandberg.html - Cached Feb 2, 2011 ... Tandberg C Series Endpoints and E/EX Personal Video units that are ... Resolving this default password issue does not require a software ...

Tandberg MXP 1000 - Password recovery|2176967 - Cisco Support ... https://supportforums.cisco.com/thread/2176967 - Cached Oct 15, 2012 ... Tandberg MXP 1000 - Password recovery Does anyone know how to recover a lost password for an MXP ... Or how to reset to factory defaults?

Technical FAQ's > Support > VSGi www.vsgi.com/support/technical_faq.php - Cached - Similar What is the default password for my videoconferencing system? For Tandberg Systems: The default password is "TANDBERG". For Polycom Systems: Use the ...

Tandberg Password Resetting To change your password ... - Visitec www.visitec.com/tand_docs/Tandberg%20Password%20Resetting.pdf - Cached - Similar Tandberg Password Resetting. To change your password on the MXP Units (newer systems) there are two ways to do this, both of these require you to be in the ...



CIRT.net

suspicion breeds confidence

Home

Default Passwords

 Search

473 vendors, 1954 passwords

Ip Scan

Scan your Business Network IP Free Network IP Scan.
[IP Scan Qualys.com](#)



AdChoices

1. Tandberg - Gatekeeper

User ID admin
Password TANDBERG
Level Administrator

2. Tandberg - Border Controller

Method Telnet/SSH/HTTP
User ID admin
Password TANDBERG
Level Administrator

3. Tandberg - Vision

Version 5000/2500/2000/800
User ID (none)
Password GWrv
Level Administrator

4. Tandberg - Codec



Nikto

- [Nikto](#)
- [Development](#)
- [Documentation](#)
- [Mail List](#)
- [Press](#)
- [Books](#)
- [Related Projects](#)
- [Products & Swag](#)

Data

- [Default Passwords](#)
- [Default Ports](#)
- [Advisories](#)

Code

- [DAVTest](#)
- [Clickjack Testing](#)
- [CMS Explorer](#)
- [svnpristine](#)
- [Site Crunch](#)
- [Iw_build_req](#)
- [MP3 Duplicate Finder](#)
- [All Projects](#)

About

- [dave](#)

Newfolk VTC

Overview Phonebook System Status System Configuration Endpoint Configuration
Front Overview Call Streaming Text Chat



WELCOME TO USCG 4TH FL CONF RM

| Dial in numbers | |
|-----------------|----------------|
| My ISDN number | 7576284132 |
| My IP number | 7579621504 |
| My IP name | 4TH FL CONF RM |
| My SIP URI | |

| Usage | |
|-----------------|-----------------------|
| Video calls | 1 of 3 |
| Telephone calls | 0 of 3 |
| ISDN channels | 0 of 4 |
| Total bandwidth | 128 kbps of 2304 kbps |

| System Information | |
|--------------------|---------------------|
| System Name | USCG 4TH FL CONF RM |
| Software version | F9.1.2 NTSC |
| Product | TANDBERG Edge 95MXP |
| Location | |
| Contact Person | |

| System Status | | |
|---------------|------------|-------------------------|
| ISDN/BRI | Line error | ● More |
| H.323 | | ●✓ More |
| SIP | | ● More |

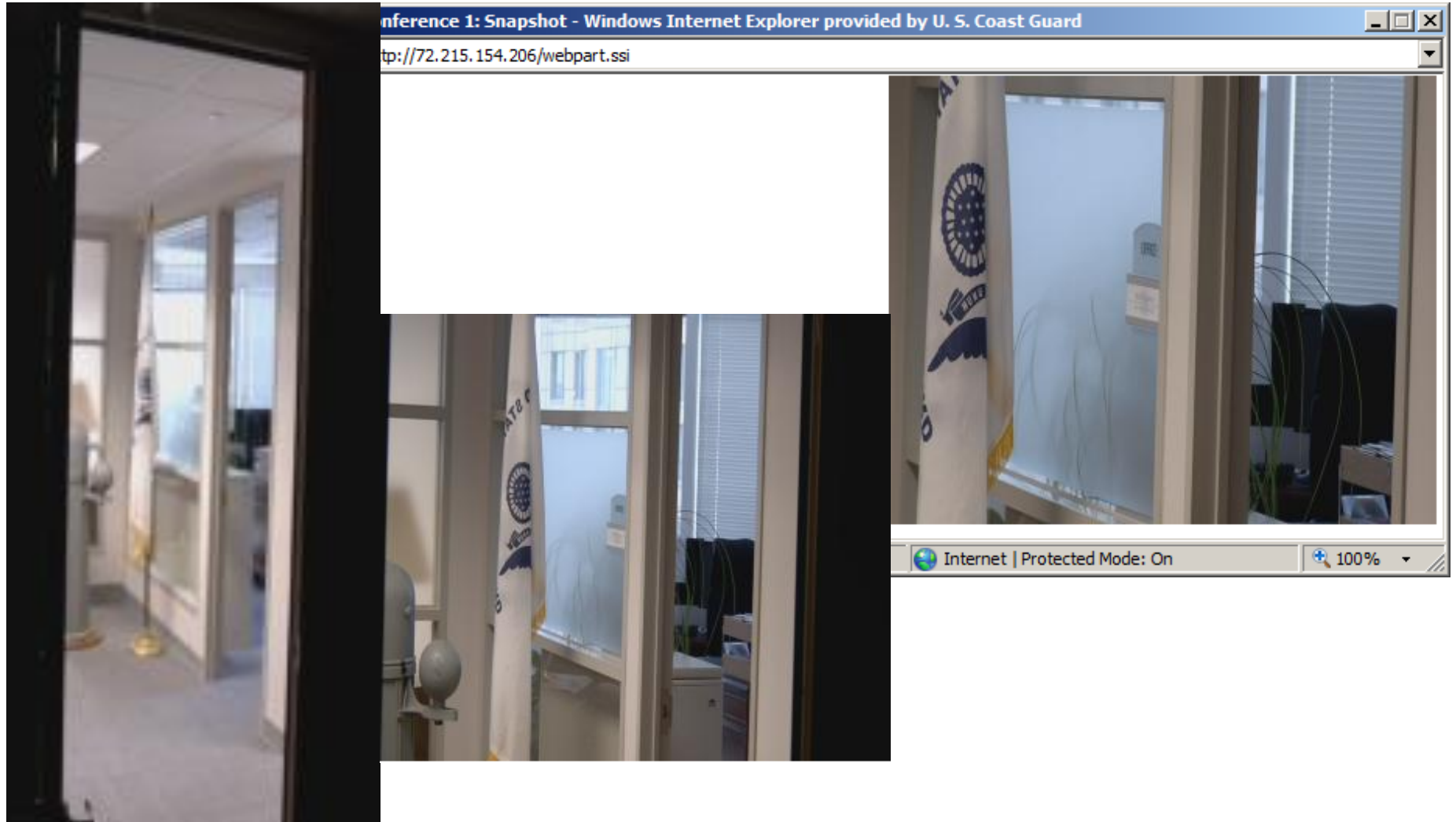
No Active Call, using camera self-



4th Deck camera control viewing office space adjacent to conference room



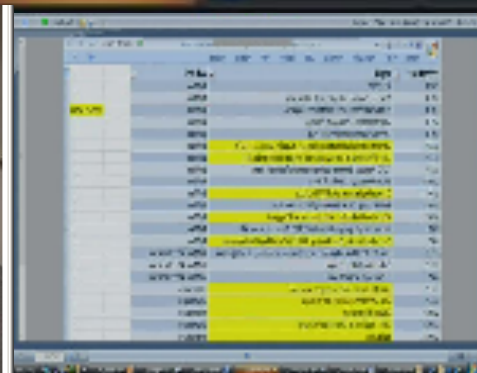
6th Deck camera control viewing office space adjacent to conference room



UNCLAS//FOUO

| Category | Topic | Breakout |
|----------|---|-----------------------|
| LREPL | Solving High Failure Rate Equipment (Supply, Maint, or TCTO) | 1) Main |
| LREPL | Lack of funding to remove gear no longer supported (C4IT) | 1) Main |
| LREPL | TCTO Process: Emphasize importance of doing it right | 1) Main |
| MECPL | EAL Pilot study: Results & Plans | 1) Main |
| MECPL | Cmplus Replacement & MAM rollout | 1) Main |
| MECPL | Reinstating Cutter Inventory/Allowance Lists | 1) Main |
| MECPL | Wellin Lambie Davits: Maintenance and Support | 1) Main |
| SBPL | Centralized Cutter Boat Pooling (CCBP) & Small Boat Maintenance | 1) Main |
| SBPL | Forward staging of parts/boats (GTMO, Guam, Boston, AK) | 1) Main |
| LREPL | One POC for Charlie Periods: Maintenance scheduling & integration | 2) Main &/or Breakout |
| LREPL | Optimizing Cutter Tempo | 2) Main &/or Breakout |
| SBPL | Cutter Boat Acquisitions | 2) Main &/or Breakout |
| LREPL | Lube Oil costs: Shift to energy account? | 3) Breakout |
| LREPL | Unit Environmental Guide Updates | 3) Breakout |
| MECPL | OVS performance | 3) Breakout |
| MECPL | Safe To Fail Lists & updates/changes | 3) Breakout |
| MECPL | Ballasting | 3) Breakout |
| MECPL | MAT/NESU Support | 3) Breakout |
| Each PLM | Platform-specific TCTO review | 3) Breakout |

6th Floor Conf 12APR13 (VTC w/SFLC)
Two days later, VTC reenabled without Default Password Change



Questions?

ACT

Achieving Cybersecurity Together
“It’s our Shared Responsibility”.

