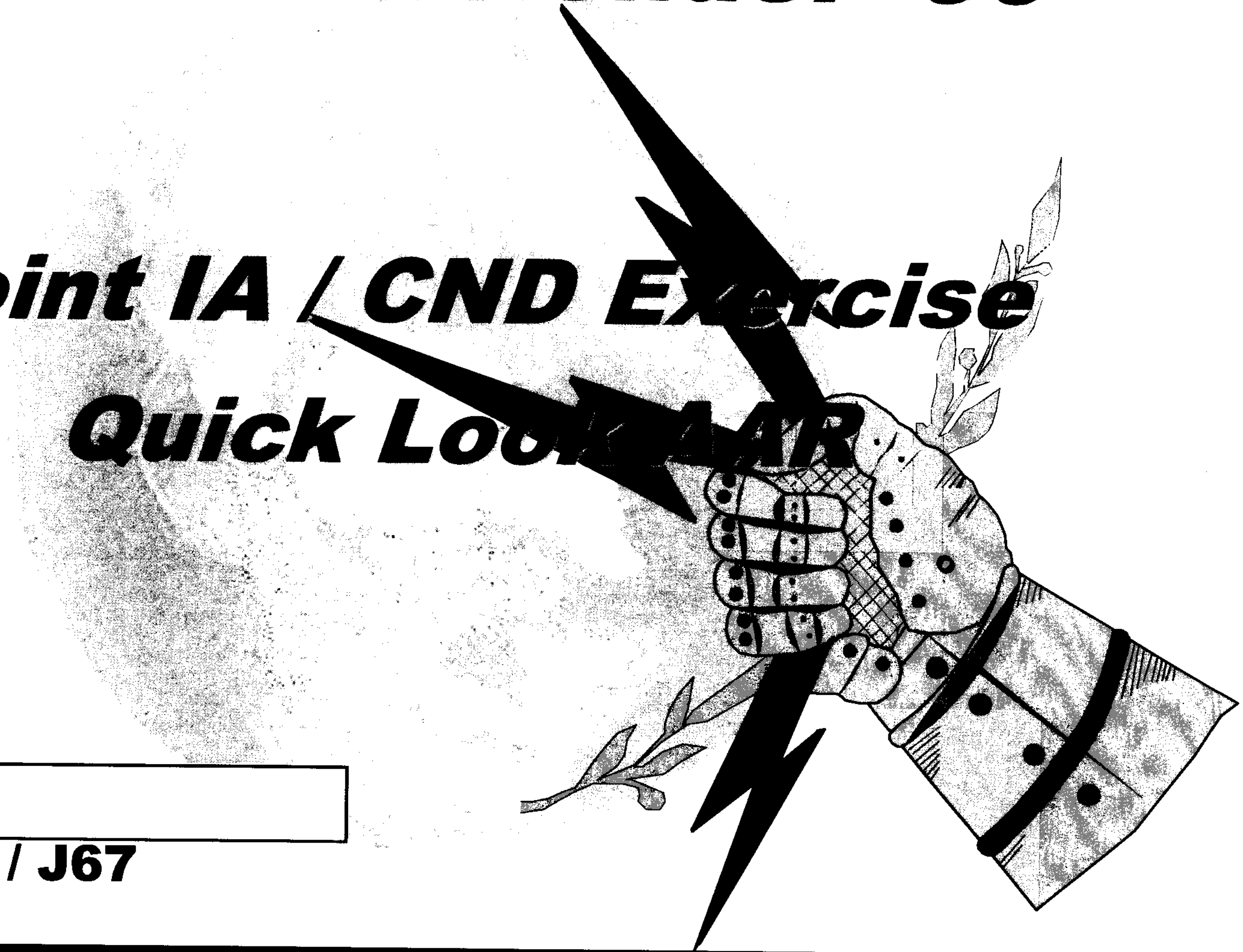
Overall Classification: ~~FOR OFFICIAL USE ONLY~~

Bulwark Defender '06



Joint IA / CND Exercise Quick Look AAR

Lt Col Non-Responsive USSC
USSTRATCOM / J67
08 Jun 06

Intent

- Assess ability of the Services, respective NOSCs and network defenders to jointly conduct IA / CND
- Exercise and validate the ability to protect DoD networks from attack while ensuring the integrity and availability of information for the warfighter
- Train DoD network defenders to decisively fight
- Confirm importance of defending networks to warfighters

Exercise Objectives

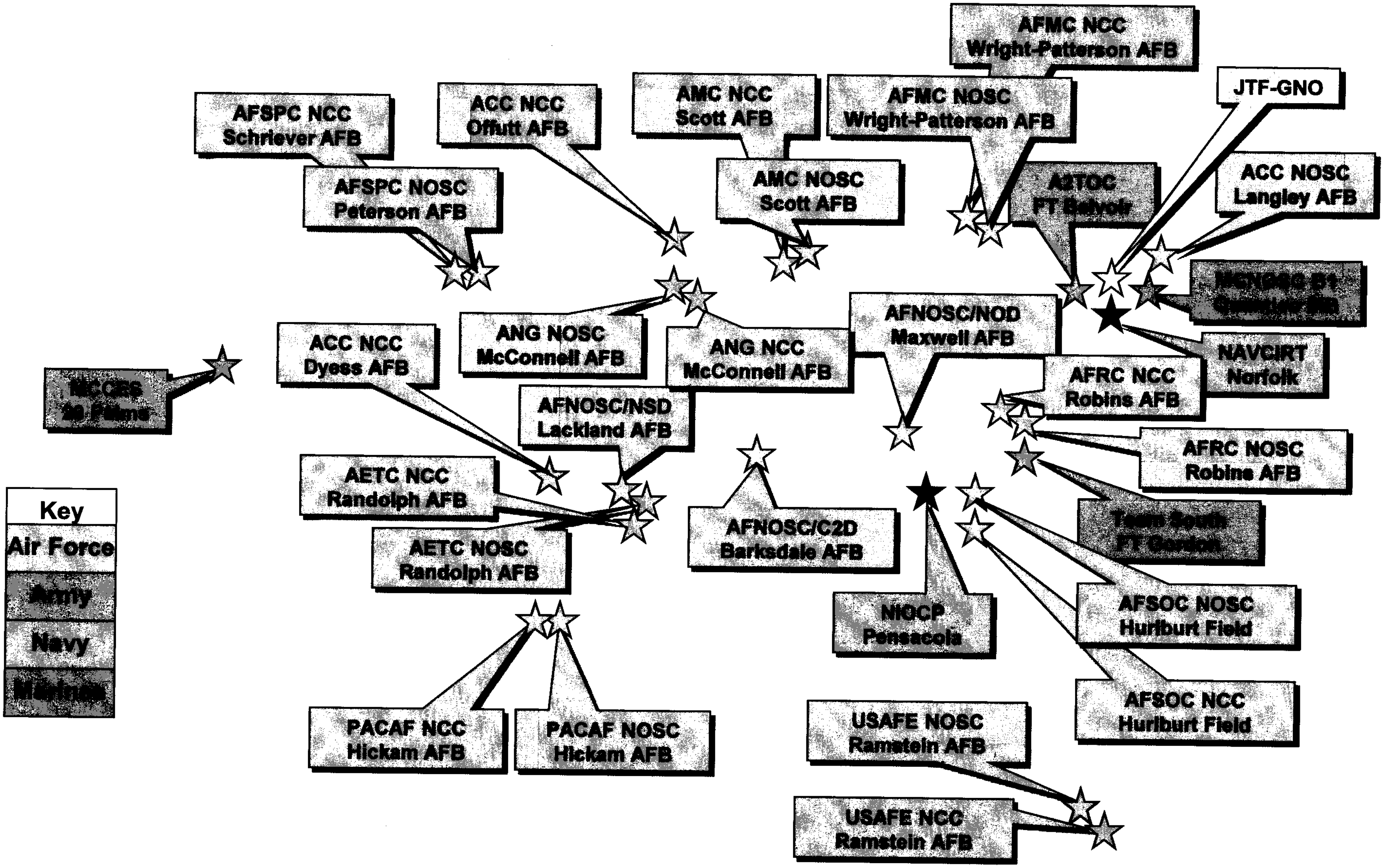
1. Train personnel to defend against a directed professional attack against the GIG

2. Train and evaluate personnel in C2 procedures and operational tactics

3. Evaluate and refine information flow/fusion/dissemination between the Service NOSCs / CERTs /JTF-GNO

4. Evaluate and refine NetOps Tactics, Techniques and Procedures

BD06 – Participating Locations



AFMC NCC
Wright-Patterson AFB

JTF-GNO

AFSPC NCC
Schriever AFB

ACC NCC
Offutt AFB

AMC NCC
Scott AFB

AFMC NOSC
Wright-Patterson AFB

AFSPC NOSC
Peterson AFB

AMC NOSC
Scott AFB

A2TOC
FT Belvoir

ACC NOSC
Langley AFB

MCNOSC S1
Quantico Va

ANG NOSC
McConnell AFB

ANG NCC
McConnell AFB

AFNOSC/NOD
Maxwell AFB

NAVCIRT
Norfolk

MCCES
29 Palms

ACC NCC
Dyess AFB

AFRC NCC
Robins AFB

AFNOSC/NSD
Lackland AFB

AFRC NOSC
Robins AFB

AETC NCC
Randolph AFB

Team South
FT Gordon

AFNOSC/C2D
Barksdale AFB

AETC NOSC
Randolph AFB

AFSOC NOSC
Hurlburt Field

NIOCP
Pensacola

AFSOC NCC
Hurlburt Field

PACAF NCC
Hickam AFB

PACAF NOSC
Hickam AFB

USAFE NOSC
Ramstein AFB

USAFE NCC
Ramstein AFB

Key
Air Force
Army
Navy
Marines

2 Week Battle Rhythm

Scenario 1
(LIVE)
Critical Data Exfiltration

Starts 45 Days prior to Range STARTEX

MARCH

SUNDAY	MONDAY	TUESDAY	WEDNESDAY	THURSDAY	FRIDAY	SATURDAY
5	6	7	8	9	10	11
TRAVEL	IN-BRIEFS OPS CHECK RANGE FAM	RANGE PLAY	RANGE PLAY	RANGE PLAY	RANGE PLAY [redacted]	RE-ROLLS **GLOBAL HOTWASH** [redacted]
12	13	14	15	16	17	18
NO PLAY [redacted]	LIVE PLAY [redacted]	LIVE PLAY	LIVE PLAY	LIVE PLAY	HOTWASH	TRAVEL

BD06 Scenario Summary

- Scenario 1 – Critical information exfiltration
- Scenario 2 – Simulated wireless SIPR compromise
- Scenario 3 – Cross-service web compromise
- Scenario 4 – AFNOSC DRP/COOP
- Scenario 5 – Misuse of network
- Scenario 8 – Cross service classified msg incident
- Scenario 9 – Hacker printer attack
- Scenario 10 – Cross service Email DOS
- Scenario 11 – Distributed Denial of Service
- Scenario 12 – Email phishing attack
- Scenario 13 – Rogue wireless device
- Scenario 14 – Total Network Takeover (TNT) – Fast
- Scenario 16 – Attempted TNT - Slow
- Scenario 17 – AF wide web attack
- Scenario 18 – Multiple NCC targeted net ops events
- Scenario 19 – AFNOSC/NOD scenario

EXERCISE BULWARK DEFENDER 06

Observations

Top 5 Take-aways

1. Enable 24x7 collaboration for agile, responsive C2, awareness, and defense
2. Build a persistent IA / CND training/exercise capability for premier defense
3. Establish baseline defense capabilities at tactical level to improve DoD CND
4. Balance efforts to restore network services and defend…to optimize both
5. Integrate offensive and defensive functions for effective, proactive NetOps

EXERCISE BULWARK DEFENDER 06

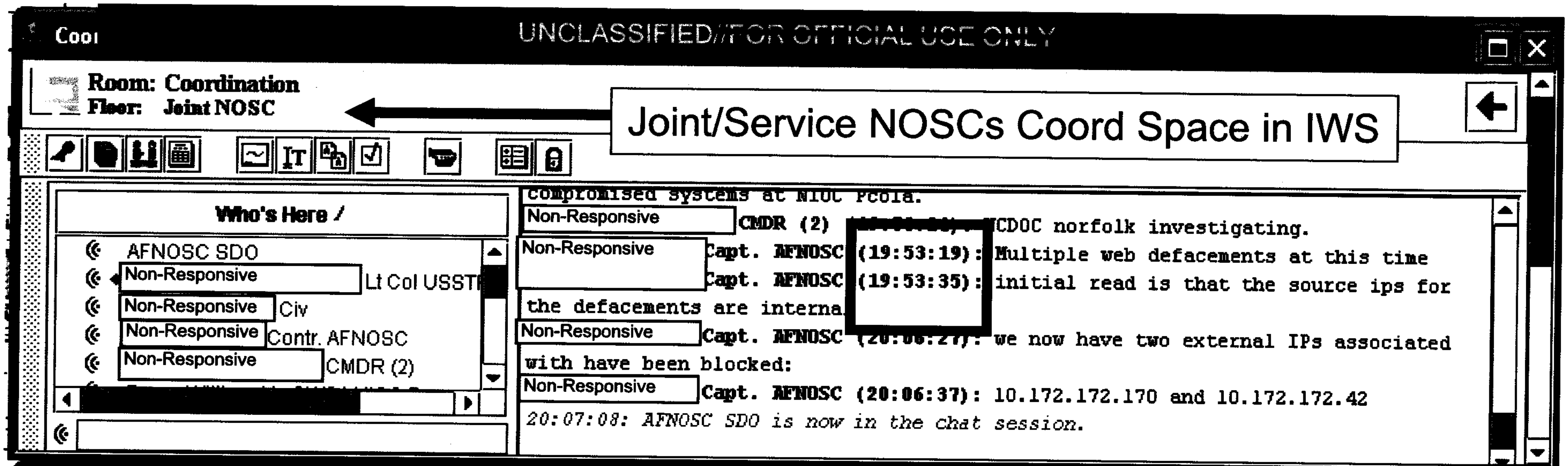
Observations

Top 5 Take-aways

1. Enable 24x7 collaboration for agile, responsive C2, awareness, and defense
    - Facilitated effective operational-tactical communications
    - Enabled awareness on enterprise-wide attacks in minutes
    - Supported near-real time correlation and response on attack events

Action: JTF-GNO, Services, DISA

UNCLASSIFIED//FOR OFFICIAL USE ONLY

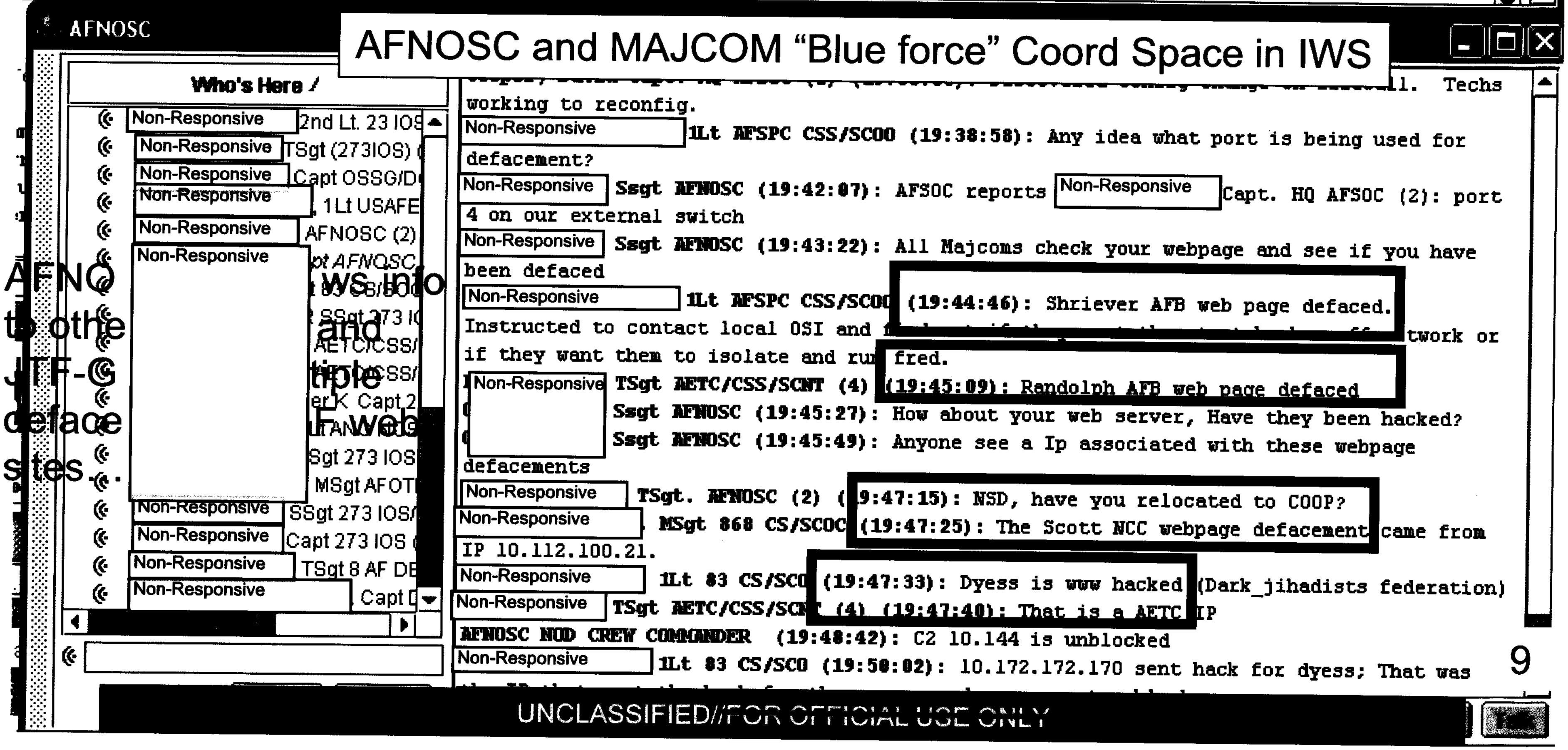


Joint/Service NOSCs Coord Space in IWS

Who's Here /

AFNOSC SDO
Non-Responsive Lt Col USST
Non-Responsive Civ
Non-Responsive Contr. AFNOSC
Non-Responsive CMDR (2)

```
compromised systems at NIOC Pcola.
Non-Responsive CMDR (2) (        ): NCDOC norfolk investigating.
Non-Responsive Capt. AFNOSC (19:53:19): Multiple web defacements at this time
Capt. AFNOSC (19:53:35): initial read is that the source ips for
the defacements are interna
Non-Responsive Capt. AFNOSC (20:06:27): we now have two external IPs associated
with have been blocked:
Non-Responsive Capt. AFNOSC (20:06:37): 10.172.172.170 and 10.172.172.42
20:07:08: AFNOSC SDO is now in the chat session.
```



AFNOSC and MAJCOM "Blue force" Coord Space in IWS

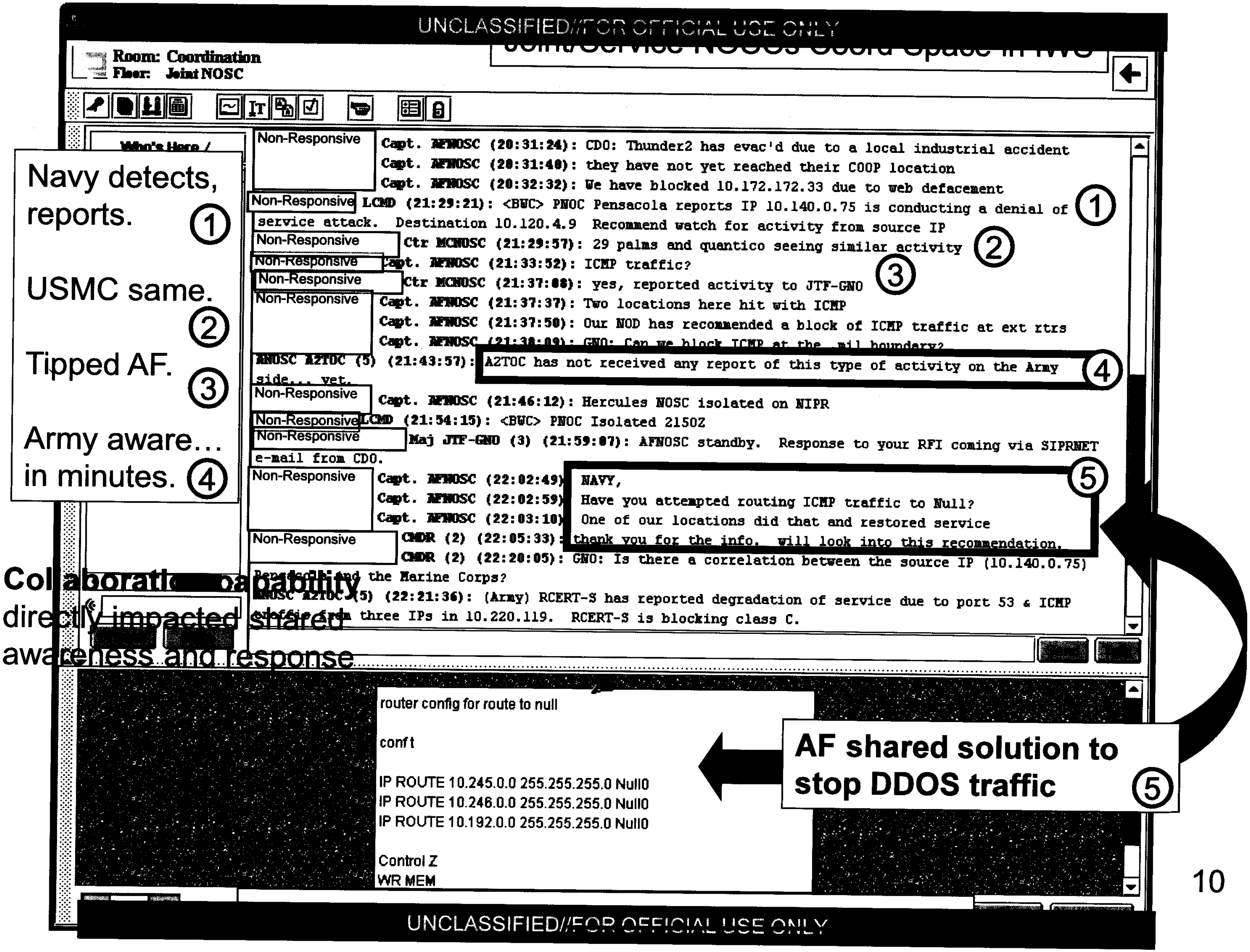
Who's Here /

Non-Responsive 2nd Lt. 23 IOS
Non-Responsive TSgt (273IOS)
Non-Responsive Capt OSSG/D
Non-Responsive 1Lt USAFE
Non-Responsive AFNOSC (2)
Non-Responsive
Non-Responsive SSgt 273 IOS/
Non-Responsive Capt 273 IOS
Non-Responsive TSgt 8 AF DE
Non-Responsive Capt

AFNO ws info
to othe and
JTF-G tiple
deface Web
sites...

```
                                                              ll.  Techs
working to reconfig.
Non-Responsive 1Lt AFSPC CSS/SCOO (19:38:58): Any idea what port is being used for
defacement?
Non-Responsive Ssgt AFNOSC (19:42:07): AFSOC reports Non-Responsive Capt. HQ AFSOC (2): port
4 on our external switch
Non-Responsive Ssgt AFNOSC (19:43:22): All Majcoms check your webpage and see if you have
been defaced
Non-Responsive 1Lt AFSPC CSS/SCOO (19:44:46): Shriever AFB web page defaced.
Instructed to contact local OSI and                                 twork or
if they want them to isolate and ru fred.
Non-Responsive TSgt AETC/CSS/SCNT (4) (19:45:09): Randolph AFB web page defaced
Ssgt AFNOSC (19:45:27): How about your web server, Have they been hacked?
Ssgt AFNOSC (19:45:49): Anyone see a Ip associated with these webpage
defacements
Non-Responsive TSgt. AFNOSC (2) ( 9:47:15): NSD, have you relocated to COOP?
Non-Responsive MSgt 868 CS/SCOC (19:47:25): The Scott NCC webpage defacement came from
IP 10.112.100.21.
Non-Responsive 1Lt 83 CS/SCO (19:47:33): Dyess is www hacked (Dark_jihadists federation)
Non-Responsive TSgt AETC/CSS/SCNT (4) (19:47:40): That is a AETC IP
AFNOSC NOD CREW COMMANDER (19:48:42): C2 10.144 is unblocked
Non-Responsive 1Lt 83 CS/SCO (19:50:02): 10.172.172.170 sent hack for dyess; That was
```

UNCLASSIFIED//FOR OFFICIAL USE ONLY



Navy detects, reports. ①

USMC same. ②

Tipped AF. ③

Army aware… in minutes. ④

```
Non-Responsive Capt. AFNOSC (20:31:24): CDO: Thunder2 has evac'd due to a local industrial accident
               Capt. AFNOSC (20:31:40): they have not yet reached their COOP location
               Capt. AFNOSC (20:32:32): We have blocked 10.172.172.33 due to web defacement
Non-Responsive LCMD (21:29:21): <BWC> PNOC Pensacola reports IP 10.140.0.75 is conducting a denial of
service attack.  Destination 10.120.4.9  Recommend watch for activity from source IP          ①
Non-Responsive Ctr MCNOSC (21:29:57): 29 palms and quantico seeing similar activity          ②
Non-Responsive Capt. AFNOSC (21:33:52): ICMP traffic?                                         ③
Non-Responsive Ctr MCNOSC (21:37:08): yes, reported activity to JTF-GNO
Non-Responsive Capt. AFNOSC (21:37:37): Two locations here hit with ICMP
               Capt. AFNOSC (21:37:50): Our NOD has recommended a block of ICMP traffic at ext rtrs
               Capt. AFNOSC (21:38:09): GNO: Can we block ICMP at the .mil boundary?
ANOSC A2TOC (5) (21:43:57): A2TOC has not received any report of this type of activity on the Army
side... yet.                                                                                   ④
Non-Responsive Capt. AFNOSC (21:46:12): Hercules NOSC isolated on NIPR
Non-Responsive LCMD (21:54:15): <BWC> PNOC Isolated 2150Z
Non-Responsive Maj JTF-GNO (3) (21:59:07): AFNOSC standby.  Response to your RFI coming via SIPRNET
e-mail from CDO.
Non-Responsive Capt. AFNOSC (22:02:49): NAVY,                                                  ⑤
               Capt. AFNOSC (22:02:59): Have you attempted routing ICMP traffic to Null?
               Capt. AFNOSC (22:03:10): One of our locations did that and restored service
Non-Responsive CMDR (2) (22:05:33): thank you for the info.  will look into this recommendation.
               CMDR (2) (22:20:05): GNO: Is there a correlation between the source IP (10.140.0.75)
Pensacola and the Marine Corps?
ANOSC A2TOC (5) (22:21:36): (Army) RCERT-S has reported degradation of service due to port 53 & ICMP
traffic from three IPs in 10.220.119.  RCERT-S is blocking class C.
```

Collaboration capability directly impacted shared awareness and response

```
router config for route to null

conf t

IP ROUTE 10.245.0.0 255.255.255.0 Null0
IP ROUTE 10.246.0.0 255.255.255.0 Null0
IP ROUTE 10.192.0.0 255.255.255.0 Null0

Control Z
WR MEM
```

AF shared solution to stop DDOS traffic ⑤

EXERCISE BULWARK DEFENDER 06

Observations

Top 5 Take-aways

2. Build a persistent IA / CND training/exercise capability for premier defense
   - Red Team-led training on tactics range—most valuable learning activity
   - Joint range allowed community effort to improve defense
   - Range supported safe ability to exercise robust NetOps scenarios
   - A standing capability to train / shape defense tactics sustains advantage
   - “Time-sensitive training” range enables responsive tactics maneuvering

Action: ASD/NII, JS/J6, USSTRATCOM, JFCOM, NSA, Services, DISA

EXERCISE BULWARK DEFENDER 06

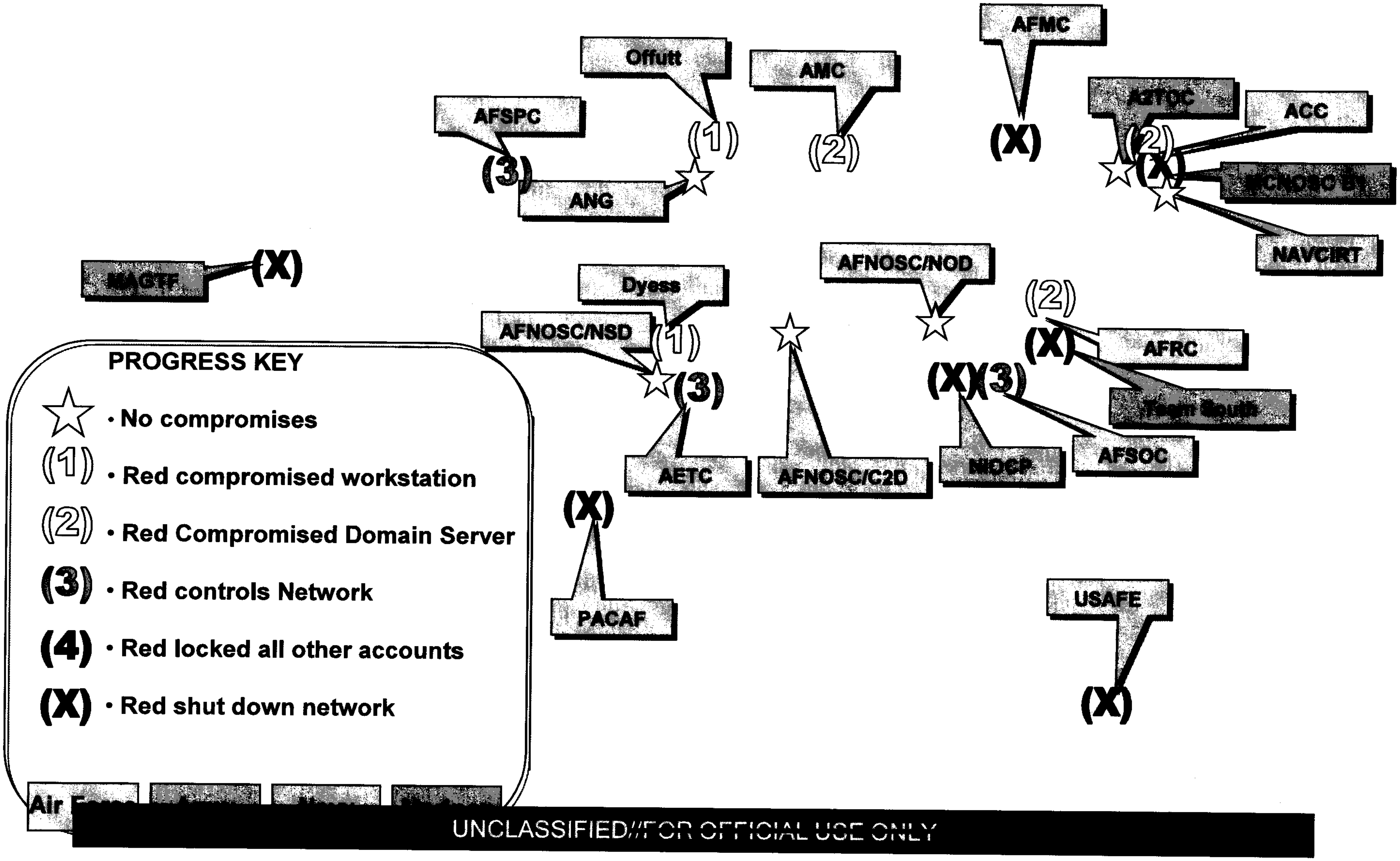
Observations

Top 5 Take-aways

3. Establish baseline defense capabilities at tactical level to improve DoD CND
   - Bases with intrusion detection, intrusion protection, and port security successfully blocked attacks
   - Signature-based intrusion detection alone was not effective
   - Some Services have acquired capabilities, but not yet fully fielded
   - User awareness remains a critical element of defense…

Action: ASD/NII, Services, USSTRATCOM

Scenario 16 Results
Cross-Service Total Network Takedown (Range)



PROGRESS KEY

- ☆ • No compromises
- (1) • Red compromised workstation
- (2) • Red Compromised Domain Server
- (3) • Red controls Network
- (4) • Red locked all other accounts
- (X) • Red shut down network

EXERCISE BULWARK DEFENDER 06

Observations

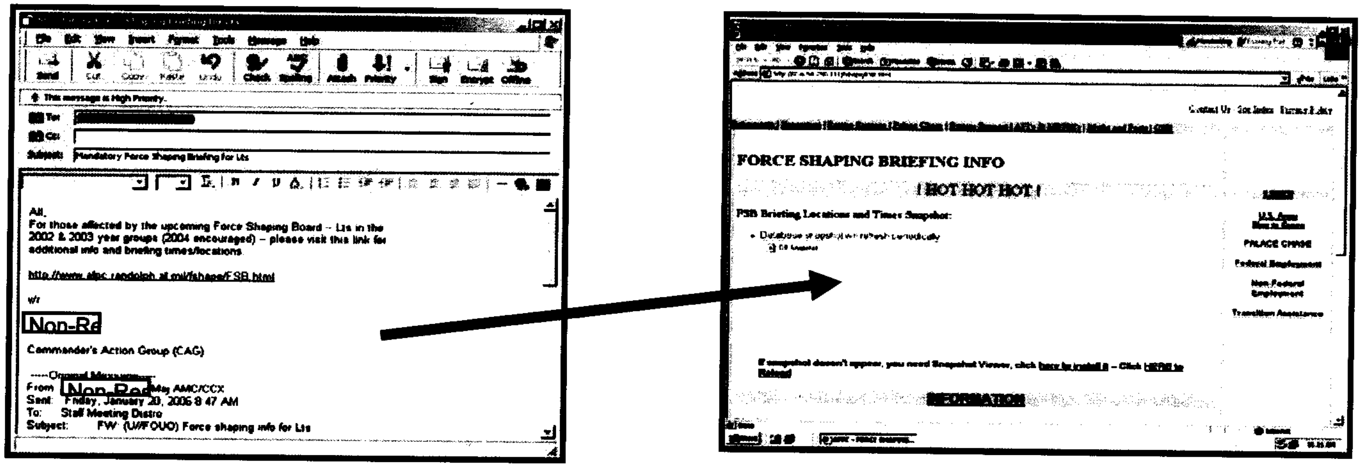
Scenario 1- Exfiltration of Critical Information

Red Objective: Access unclassified AF networks and mine / copy critical data

Targets: AFNOSC, MAJCOM NOSCs and participating NCCs

Attack vector:

- Use phishing emails to gain access to a computer
- Use compromised computer to gain access / control of network


File Edit View Insert Format Tools Message Help
Send Cut Copy Paste Undo Check Spelling Attach Priority Sign Encrypt Offline

This message is High Priority.

To: [redacted]

Cc:

Subject: Mandatory Force Shaping Briefing for Lts

All,
For those affected by the upcoming Force Shaping Board -- Lts in the 2002 & 2003 year groups (2004 encouraged) – please visit this link for additional info and briefing times/locations

http://www.afpc.randolph.af.mil/fshape/FSB.html

v/r

Non-Re

Commander's Action Group (CAG)

-----Original Message-----
From: Non-Red Maj AMC/CCX
Sent: Friday, January 20, 2006 8:47 AM
To: Staff Meeting Distro
Subject: FW: (U//FOUO) Force shaping info for Lts

FORCE SHAPING BRIEFING INFO

! HOT HOT HOT !

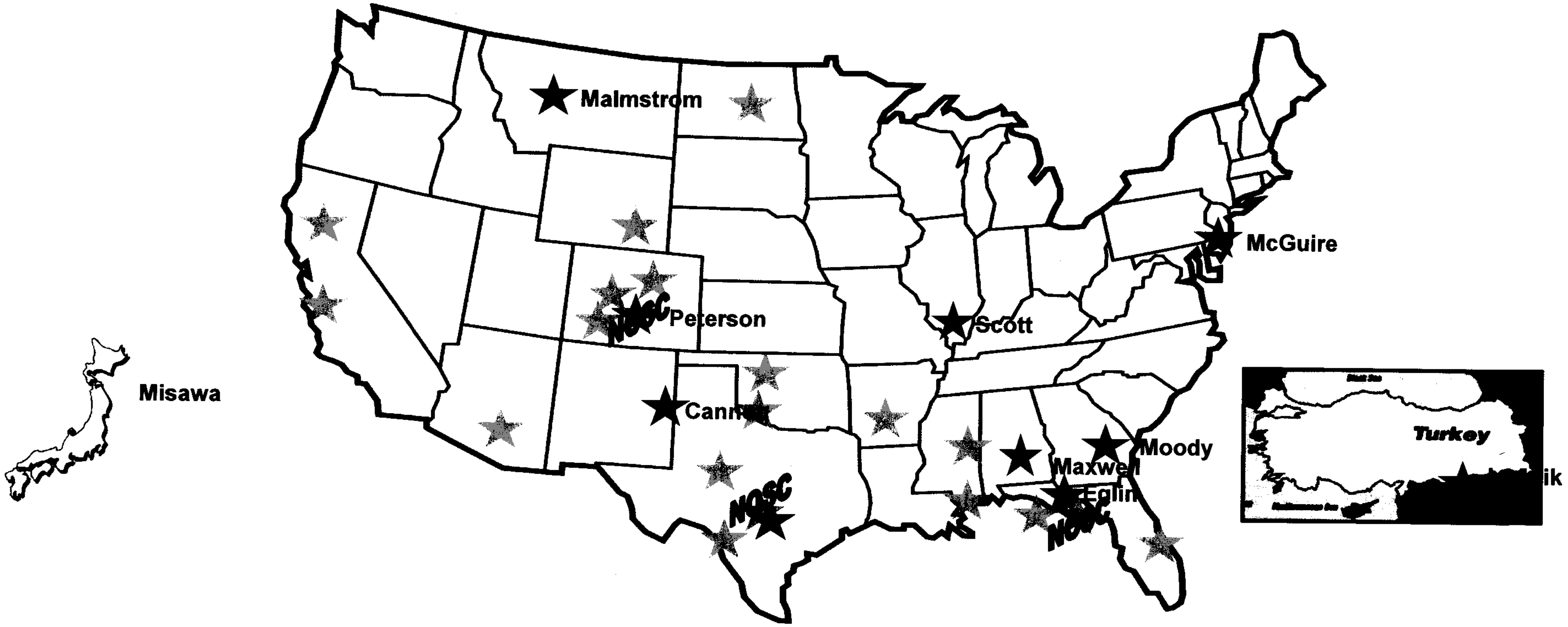
FSB Briefing Locations and Times Snapshot:

- Database snapshot will refresh periodically

If snapshot doesn't appear, you need Snapshot Viewer, click here to install it – Click HERE to Reload

INFORMATION

Scenario 1 Results (AF)
Exfiltration of Critical Information



★ Primary Compromise

★ Secondary Compromise

★ Red Team HQ

Presence on 9 Bases

Control of 3 Enterprises

EXERCISE BULWARK DEFENDER 06

Observations

Top 5 Take-aways

4. Balance efforts to restore network services and defend…to optimize both
   - "We are training more of a service provider than a network defender"
   - Many defenders focused on restoring service at the expense of defense
   - "Defense-focused" defenders effectively stopped attacks

Action: ASD/NII, USSTRATCOM, Joint Staff, Services, JFCOM, DISA

EXERCISE BULWARK DEFENDER 06

Observations

Top 5 Take-aways

5. Integrate offensive and defensive functions for effective, proactive NetOps
   - Co-located, integrated NetOps functions are effective
   - Unity of effort is required between offensive and defensive NetOps communities to achieve and sustain advantage
   - Shared awareness of activities, events, and capabilities across CNA / CNE / CND communities promises economies and superiority
   - Indications & warnings enables proactive defense
   - Integrated CNA / CNE / CND is required for dominant NetOps

Action: ASD/NII, Services, USSTRATCOM (JTF-GNO, JFCC-NW), JS, NSA, IC

EXERCISE BULWARK DEFENDER 06

Observations

Top 5 Take-aways

Initial Recommendations:

- Establish 24/7 collaboration capability between key NetOps / network defense sites and JTF-GNO
- Achieve and resource a persistent IA / CND training capability
- Advance efforts to acquire and operate baseline tactical-level capabilities enterprise-wide to detect, defend, and respond to attacks
- Improve relationships and flow of information between I&W providers and NetOps community
- Exercise, validate, improve integrated offensive defensive NetOps

EXERCISE BULWARK DEFENDER 06

Observations

Defense Capabilities

- Persistent IA / CND training/exercise capability required for premier defense
- Tactical level functions require improved defense capabilities
- Automated patching capabilities required to improve vulnerability mgt
- Active, full-time scanning of wireless devices necessary for effective defense
- Must have local on-site personnel to isolate, t/shoot local technical problems

EXERCISE BULWARK DEFENDER 06

Observations

C2 and Information Flow

- Collaboration required for agile, responsive C2, awareness, and response
- Communications between operational and tactical levels vital to response
- Co-located, integrated NetOps, defense and warfare functions are effective
- Adjust reporting in response to increase in threat environment
- Employ / refine current INFOCON guidance for efficient enterprise defense
- Must coordinate NetOps and defense via secure communications
- Improve use of network intelligence and I&W for agility, speed in NetOps

EXERCISE BULWARK DEFENDER 06

Observations

Tactics, Techniques, Procedures

- Better balance is required between efforts to restore service and defend
- Educate defenders on types of Red scans and appropriate responses
- Clarify ROE to deconflict law enforcement and network defense
- Enforce baseline password management of network printers
- Document, coordinate COOP procedures, including reporting for execution

Way Ahead for BD07

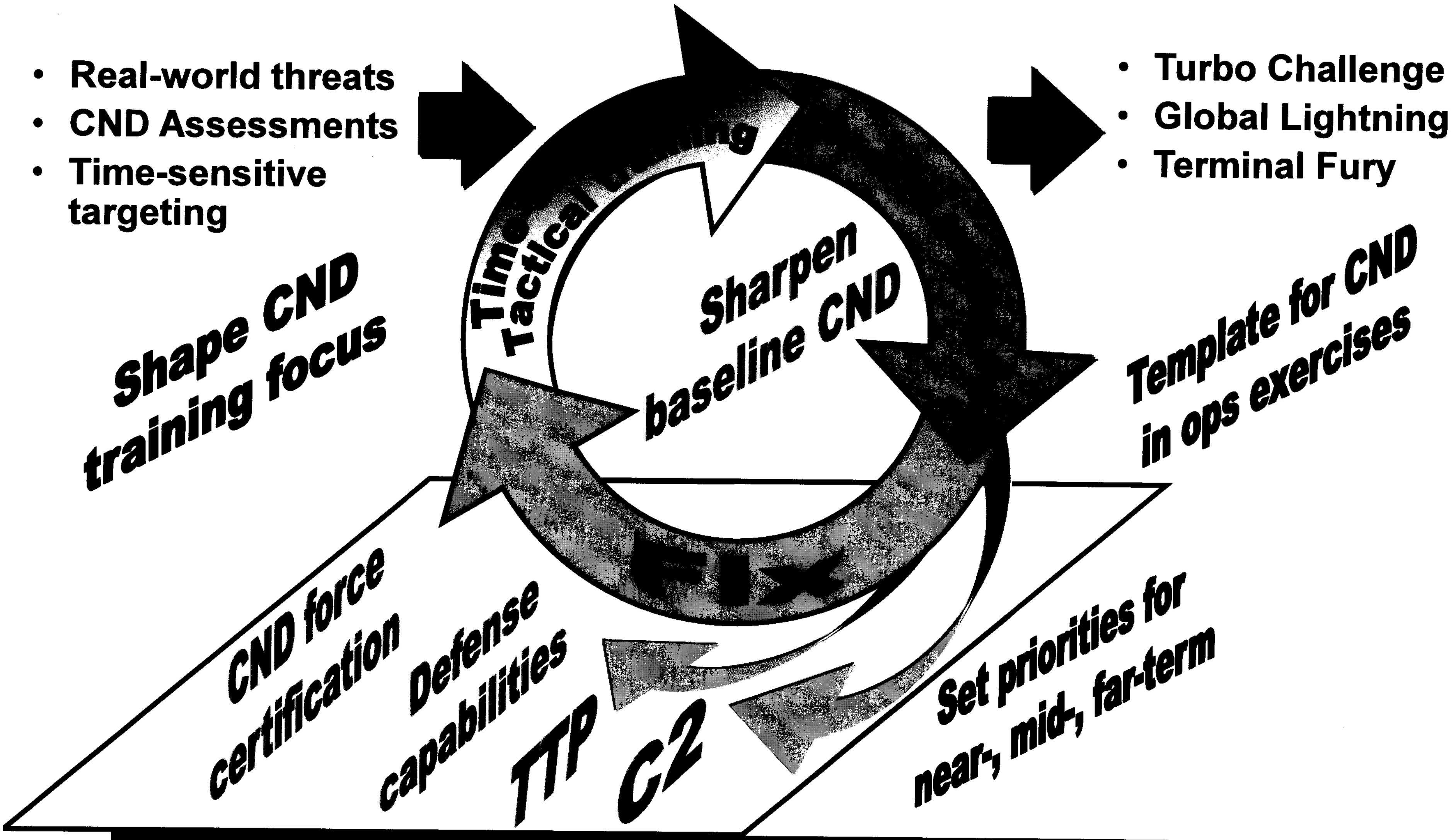
- BULWARK DEFENDER remains annual joint CND capstone event
    - Aligning BULWARK DEFENDER with GLOBAL STORM in '07
    - Execution includes focused tactics training by joint Red Team
- Using BD scenarios as template for CND events in other select exercises
- Leveraging BD lessons to shape, prioritize near-term efforts to improve joint network defense capabilities, C2, and TTP
- Continuing team effort with Joint Staff for permanent joint CND range
    - Requirement document and CONOPs
    - Potential to link with IO range
- Synchronizing with joint training capability program
- Help shape priorities and more balance for IA spending across GIG

Bulwark Defender

Capstone Joint IA / CND Event

- Real-world threats
- CND Assessments
- Time-sensitive targeting

- Turbo Challenge
- Global Lightning
- Terminal Fury



Shape CND training focus

Sharpen baseline CND

Template for CND in ops exercises

CND force certification

Defense capabilities

TTP

C2

Set priorities for near-, mid-, far-term

Bulwark Defender 07
Design Considerations

- Drive operations effects…enterprise-level
- Bring CND piece to operations exercises
  - Linkages to National, Regional, Theater, Functional levels
- Integrate, synchronize with operations storyline
  - PACOM road to war, supported by TRANSCOM, STRATCOM
- Conduct Red Team-led tactics training up front
- Emphasize free play--SIPR and NIPR, range events—in that order
- Aim for 24x7 operations
- Arrange NMCI participation
- Invite COCOMs to participate
- Promote activities to integrate offensive and defensive NetOps
- Exercise INFOCONs…TROs
- Leverage network sensors and I&W
- Staff CND JECC – guide and control support to ops exercise JECG

BD07 Exercise Linkages

Ongoing Real World Ops (OIF/OEF, GWOT, "Seams" etc.)

National

Joint Staff
National-Strategic Mobilization, Deployment CPX

Regional

PACOM
Logistics/Sustainment, Force Flow CPX

Theater

[redacted]

Functional

(TURBO CHALLENGE 07)
Global Reach Laydown

Functional

STRATCOM (GLOBAL STORM 07)
IMD, ISR, Space Support, IO CPX, BULWARK

EXERCISE BULWARK DEFENDER 06

Questions ?

Bulwark Defender 07

AF Objectives

- Exercise AF ability to surge on the live network
- Exercise AF ability to maintain identified baselines
- Exercise AF response to real world intrusion sets
- Exercise AF response to bolt out of the blue attack
- Exercise physical security and operational impacts in conjunction with GS07
- Explore using Tactical comm
- Exercise MCCC and C2 relationship
- Exercise all new AFNETOPS relationships
- Force commanders to participate at the joint and AF level
- Exercise INFOCON levels
- Exercise local COOP for PACAF, AFSPC, AFNOSC/C2D/NSD/NOD, ACC
- Exercise TIER 1 and 2 CND/RA requests
- Exercise AF response to direct targeting of AFNETOPS C2 Structure

■ Area covered
□ Partially covered
▨ Not covered

Threats (scenarios) - Joint

	OPERATE			DEFEND		RESPOND	
FUNCTIONS / MEASURES	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	▨	▨	□ 8	▨	▨	▨	▨
Identity Authentication & Authorization	▨	■	▨	■	▨	□ 1	▨
Education Training & Awareness	■	■	■	■	▨	■	▨
Security Operations & Administration	■	▨	■	■	■	■	■
Info System Security Services	■	▨	■	■	▨	■	▨
OVERALL ASSESSMENT							

Defense Capabilities - Joint

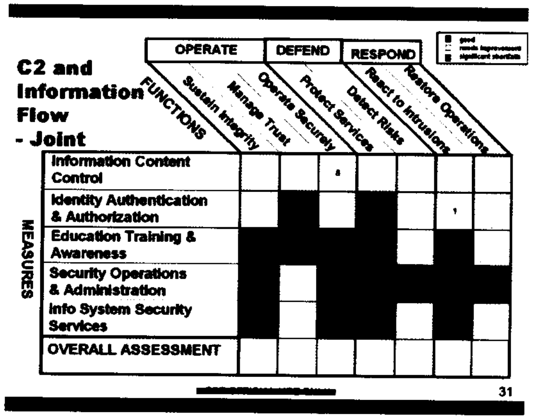
▨ good
□ needs improvement
■ significant shortfalls

MEASURES

	OPERATE			DEFEND		RESPOND	
FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	▨	▨	□ 8	▨	▨	▨	▨
Identity Authentication & Authorization	▨	■	▨	■	▨	□ 1	▨
Education Training & Awareness	■	■	■	■	▨	■	▨
Security Operations & Administration	■	▨	■	■	■	■	■
Info System Security Services	■	▨	■	■	▨	■	▨
OVERALL ASSESSMENT							

EXERCISE BULWARK DEFENDER 06

Assessment Framework

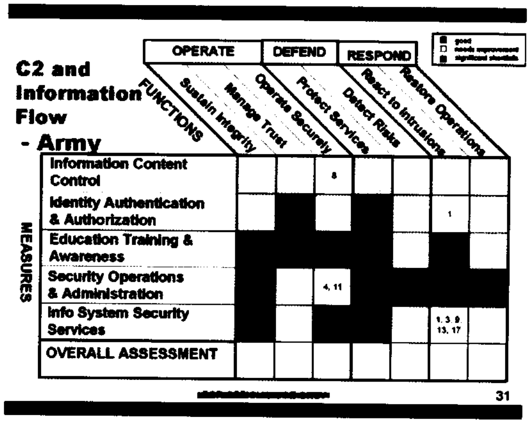


C2 and Information Flow - Joint

■ good
□ needs improvement
■ significant shortfalls

	OPERATE			DEFEND		RESPOND	
MEASURES / FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	□	□	8	□	□	□	□
Identity Authentication & Authorization	□	■	□	■	□	1	□
Education Training & Awareness	■	■	■	■	□	■	□
Security Operations & Administration	■	□	■	■	■	■	■
Info System Security Services	■	□	■	■	□	■	□
OVERALL ASSESSMENT	□	□	□	□	□	□	□

[illegible] 31

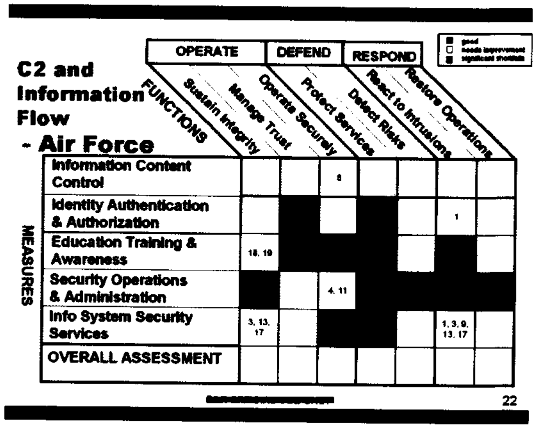


C2 and Information Flow - Army

■ good
□ needs improvement
■ significant shortfalls

	OPERATE			DEFEND		RESPOND	
MEASURES / FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	□	□	8	□	□	□	□
Identity Authentication & Authorization	□	■	□	■	□	1	□
Education Training & Awareness	■	■	■	■	□	■	□
Security Operations & Administration	■	□	4, 11	■	■	■	■
Info System Security Services	■	□	■	■	□	1, 3, 9, 13, 17	□
OVERALL ASSESSMENT	□	□	□	□	□	□	□

[illegible] 31

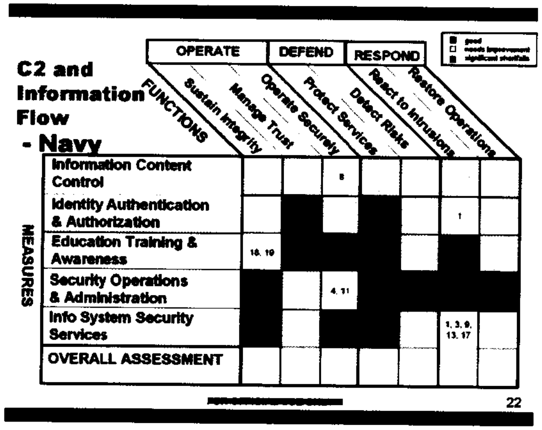


C2 and Information Flow - Air Force

■ good
□ needs improvement
■ significant shortfalls

	OPERATE			DEFEND		RESPOND	
MEASURES / FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	□	□	8	□	□	□	□
Identity Authentication & Authorization	□	■	□	■	□	1	□
Education Training & Awareness	18, 19	■	■	■	□	■	□
Security Operations & Administration	■	□	4, 11	■	■	■	■
Info System Security Services	3, 13, 17	□	■	■	□	1, 3, 9, 13, 17	□
OVERALL ASSESSMENT	□	□	□	□	□	□	□

[illegible] 22

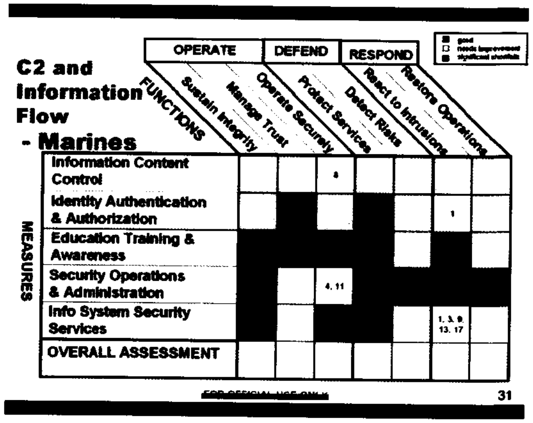


C2 and Information Flow - Navy

■ good
□ needs improvement
■ significant shortfalls

	OPERATE			DEFEND		RESPOND	
MEASURES / FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	□	□	8	□	□	□	□
Identity Authentication & Authorization	□	■	□	■	□	1	□
Education Training & Awareness	18, 19	■	■	■	□	■	□
Security Operations & Administration	■	□	4, 11	■	■	■	■
Info System Security Services	■	□	■	■	□	1, 3, 9, 13, 17	□
OVERALL ASSESSMENT	□	□	□	□	□	□	□

[illegible] 22



C2 and Information Flow - Marines

■ good
□ needs improvement
■ significant shortfalls

	OPERATE			DEFEND		RESPOND	
MEASURES / FUNCTIONS	Sustain Integrity	Manage Trust	Operate Securely	Protect Services	Detect Risks	React to Intrusions	Restore Operations
Information Content Control	□	□	8	□	□	□	□
Identity Authentication & Authorization	□	■	□	■	□	1	□
Education Training & Awareness	■	■	■	■	□	■	□
Security Operations & Administration	■	□	4, 11	■	■	■	■
Info System Security Services	■	□	■	■	□	1, 3, 9, 13, 17	□
OVERALL ASSESSMENT	□	□	□	□	□	□	□

FOR OFFICIAL USE ONLY 31

BD06 Scenario Summary

- Scenario 1 – Critical information exfiltration
- Scenario 2 – Simulated wireless SIPR compromise
- Scenario 3 – Cross-service web compromise
- Scenario 4 – AFNOSC DRP/COOP
- Scenario 5 – Misuse of network
- Scenario 8 – Cross service classified msg incident
- Scenario 9 – Hacker printer attack
- Scenario 10 – Cross service Email DOS
- Scenario 11 – Distributed Denial of Service
- Scenario 12 – Email phishing attack
- Scenario 13 – Rogue wireless device
- Scenario 14 – Total Network Takeover (TNT) – Fast
- Scenario 16 – Attempted TNT - Slow
- Scenario 17 – AF wide web attack
- Scenario 18 – Multiple NCC targeted net ops events
- Scenario 19 – AFNOSC/NOD scenario

Scenario	Live Net	Range Net
1	AF, MC	A, N
2	AF, MC, A	
3		AF, MC, A, N
4	AF	
5	AF, MC, A	N
8	AF, MC, A	AF, N
9	AF, MC	A, N
10		AF, A, N
11		AF, A, N, MC
12	AF, MC, N	
13	AF, MC	
14		AF, A
16		AF, A, MC, N
17		AF
18		AF, A, MC, N
19		AF

EXERCISE BULWARK DEFENDER 06

Observations

Take-aways for Way Ahead

- Joint IA / CND exercise serves as significant basis for improving joint NetOps
- Integrated CNA / CNE / CND play is required to fully exercise NetOps
- Based on recognized value—Navy plans to extend future play to shore commands, Fleet units, Navy networks (NMCI, ONENET, IT-21)
- USMC - exercising and coordinating with a “deployed” site proved beneficial
- USMC - range events increased attention to basic incident response
- USN - range enabled validation of watch officer responses, certification
- Army - exercise significant; play must include major commands, select posts
- Include JTF-GNO in range play
- Add NMCI in next exercise