

CYBER WARGAME 13

Working Seminar - June 3-7, 2013

Jacob E. Smart Building
Conference Center
1359 Arkansas Dr.
Joint Base Andrews, MD 20762



Welcome Package

Table of Contents

Cyber WarGame Overview.....	5
Background.....	5
WarGame Mission.....	5
WarGame Objectives.....	5
WarGame Outputs	5
Event Highlights	6
Seminar Events Overview	Error! Bookmark not defined.
Cyber Policy Seminar	6
Future Cyber Environment Seminar	6
Cyber Operations Seminar	7
Seminar Construct.....	Error! Bookmark not defined.
Attendance Requirements for Cyber WarGame Events	8
Joint Base Andrews, Jacob E. Smart Area Map	10
Cyber WarGame Security Plan.....	11
Telephone Directory	11
Directions.....	12
Driving directions	12
Map of Smart Center Facility	13
Food.....	14
Coffee service	14

UNCLASSIFIED ~~FOR OFFICIAL USE ONLY (FOUO)~~

UNCLASSIFIED ~~FOR OFFICIAL USE ONLY (FOUO)~~

Cyber WarGame 13 Overview

Background

United States Cyber Command (USCYBERCOM) plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains; ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. In order to achieve this mission, the command recognizes the value in providing a forum for key military, government, and business stakeholders to explore all aspects of the future cyber threat environment and its impact on the current cyber workforce plan, Command and Control (C2) processes and enabling policy constructs.

Over the course of this summer, USCYBERCOM will conduct Cyber WarGame 13, a tabletop-execution event preceded by a series of working-seminars, all designed to identify potential solutions for the cyberspace vulnerabilities that our nation and our allies will likely face in the future. The seminars and execution for this inaugural event will be held June 3-7 and August 19-23, respectively, at the Jacob E. Smart building located at Joint Base Andrews in Maryland.

WarGame Mission

Cyber WarGame 13 (CW13) will characterize the joint cyber resource and operational requirements for the 2018 epoch in order to assist the Services in fulfilling their Title 10 responsibilities to organize, train, and equip forces for employment by Unified Commanders around the world.

WarGame Objectives

- Analyze the planned Cyber Mission Force (CMF) laydown, employment concepts, and C2 constructs and an equivalent expected adversarial cyber battle plan
- Analyze wartime authorities, Rules of Engagement, ITO development and approval processes
- Explore future friendly and adversary cyber environment and their impacts on cyber operations
- Identify future policy and coordination constraints in the cyber realm
- Identify cyber tools, capabilities, and their recommended resource providers necessary to conduct cyber operations from ISR through operations to BDA in the future cyber environment

WarGame Outputs

- Recommendations for Joint Cyber Doctrine development
- Recommendations for future Cyber Mission Force operational C2 and force structure requirements
- Recommended authorities required to effectively conduct wartime cyber operations
- A recommended list of cyber capabilities, tools, and supporting policies necessary to conduct cyber operations
- Recommendations to more effectively identify requirement solutions
- Development of the future cyber environment and an established baseline for follow-on iterations of the Cyber WarGame Series (Cyber WarGame 14)
- Recommended inputs to USCYBERCOM's training exercises (Cyber Flag/Guard/Knight)

Event Dates

- 3-7 June: Cyber WarGame 13 Working-Seminar (Cyber Policy, Environment, Operations)
- 19-23 August: Cyber WarGame 13 Execution
- 24-26 September: Cyber WarGame 13 AAR

Working-Seminar Overview

CW13 consists of a working-seminar week culminating in a capstone WarGame event. The working-seminars are designed to explore specific aspects of the future cyber environment, policy, and operations. Each seminar topic includes a specific set of objectives and desired outputs which will feed into the larger capstone WarGame.

June 3: Cyber Environment

June 4: Cyber Environment & Policy

June 5: Cyber Policy

June 6: Cyber Operations

June 7: Cyber Operations (half-day)

The working-seminar sessions will span 0830 to 1700 each day.

A summary overview for each Seminar topic is provided below:

Cyber Environment

Purpose: Identify Explore and define the future Cyber environment for the 2018 timeframe

Objectives:

- Identify characteristics of the future cyber environment to include architecture, components, and data flow. (What does it look like?)
- An assessment of the utilization and corresponding vulnerabilities associated with the future cyber environment (How will it be used as well as exploited?)
- An assessment of the impact on future cyber operations from a US and adversarial perspective (How does the future cyber environment change how we will fight?)

Output:

- A future Cyber Environment with assessed impacts to military and commercial users.
- Inputs to policy and capability requirements to be explored in follow-on seminars
- Inputs to a future M&S construct to assist in future cyber assessments and requirements generation.

Cyber Policy

Purpose: Identify required policy and legal requirements to enable future cyber operations.

Objectives:

- Develop a policy and legal framework to address necessary authorities in support of future cyber operations.

Output:

- A legal and policy framework to enable desired cyber operations.
- Inputs to a future M&S construct to assist in future cyber decision making and assessments.

Cyber Operations

Purpose: Refine Command and Control constructs and identify cyber capabilities necessary to support future cyber operations.

Objectives:

- Assess the feasibility and utility of candidate cyber capabilities to support future cyber operations.
- Explore how candidate cyber capabilities would enable and/or impact future cyber operations.
- Identify requirements necessary to develop, optimize and operationalize the concepts.

Output:

- A set of assessed future cyber capabilities
- An outline of how cyber capabilities would impact future cyber operations
- A list of recommended way ahead for cyber capability development

Attendance Requirements for Cyber WarGame Working-Seminar

1. **Registration:** To register for the working-seminar, please visit: <https://www.fbcinc.com/e/WarGame/> If you have any problems, please contact [redacted]

[redacted] Please provide your name, organization, contact information and the dates that you are planning to attend. Also please provide a recommended role or subject matter expertise you will be providing for each event.

2. **Security requirements for Cyber WarGame:** Security clearance requirements must be fulfilled prior to event access. Presentations break-out sessions, and discussions for CYBER WARGAME 13 will range from **TOP SECRET REL FVEY** to **UNCLASSIFIED**.

Security clearances must be received by **NLT MAY 27th**. All Security clearances must be verified with the USCYBERCOM SSO prior to attendance of the WarGame event.

DoD Participants:

- DoD security managers with JPAS can send their attendee's clearances via JPAS to SMO Code "SSO CYBER." Please cite the term "Cyber Wargame - 13" in the POC Block. The Security POC block can be left vacant.

Non-DoD Participants:

- Entities and private industry security officials can fax clearance certification memorandums to: HQ USCYBERCOM/SSO, Attn: [redacted]

FVEY personnel must also send AMHS/Criticom message containing all security clearance information and the message must also include FVS (Foreign Visit System) Case Number.

Contact [redacted] USCYBERCOM/SSO office, at [redacted] If you have questions. He can also be reached via email at: [redacted]. Reference each Cyber WarGame Event that you plan to attend in your communications with him.

3. **Arrival and Departure Information:**

- All events for the Cyber WarGame Series will be held at the Jacob E. Smart building located at Joint Base Andrews, MD. The facility is located next to the Billeting Office. Jacob E. Smart building does not open its doors until 0745. Participants will not be permitted in the building until such time. Participants are expected to be on time to register, receive team assignments and badges. Participants must wear badges while in the facility during the event. Each event will start at 0830 of the event day.
- Please pay in advance for lunch, coffee and refreshments through the registration website or in person at the registration desk.

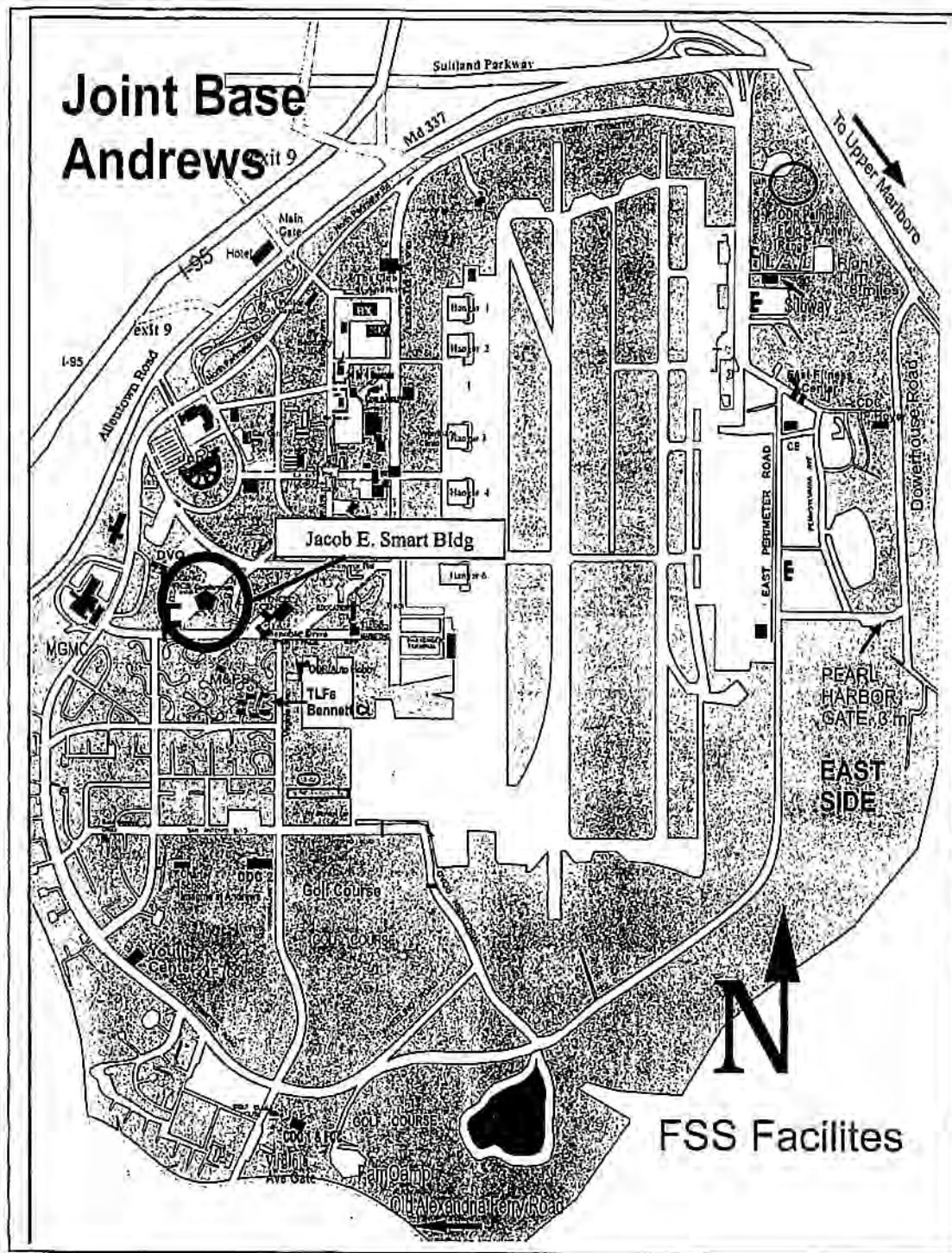
~~UNCLASSIFIED FOR OFFICIAL USE ONLY (FOUO)~~

- c. Parking is available for attendees in the parking lot in front of the Smart building facility.
- d. Participants should plan to travel on the day prior to and day after the conclusion of each specific event.



Jacob E. Smart Building

Smart Center Area Map



Cyber WarGame Security Plan

1. **OPERATIONS SECURITY (OPSEC).** The CYBERCOM managers are responsible for CYBER Wargame Critical Items (CIs) and the OPSEC program. Each participant is responsible for safeguarding their own CIs.
2. **CONFERENCE CLASSIFICATION:** Cyber WarGame will be held up to TS REL FVEY level. Participants are responsible for monitoring their discussions and maintaining them at the appropriate classification levels. Classified discussions are only allowed within the specified team rooms during the event. Participants are responsible for ensuring all classified notes are maintained at the appropriate level and that no classified material is removed from the event location.

(b) (3) 10 U.S.C. §130b
(b) (6)

Telephone Directory

Office	Name	Phone (comm)	Title	e-mail address
Jacob E. Smart Bldg	Main	240-612-6500		

Note:

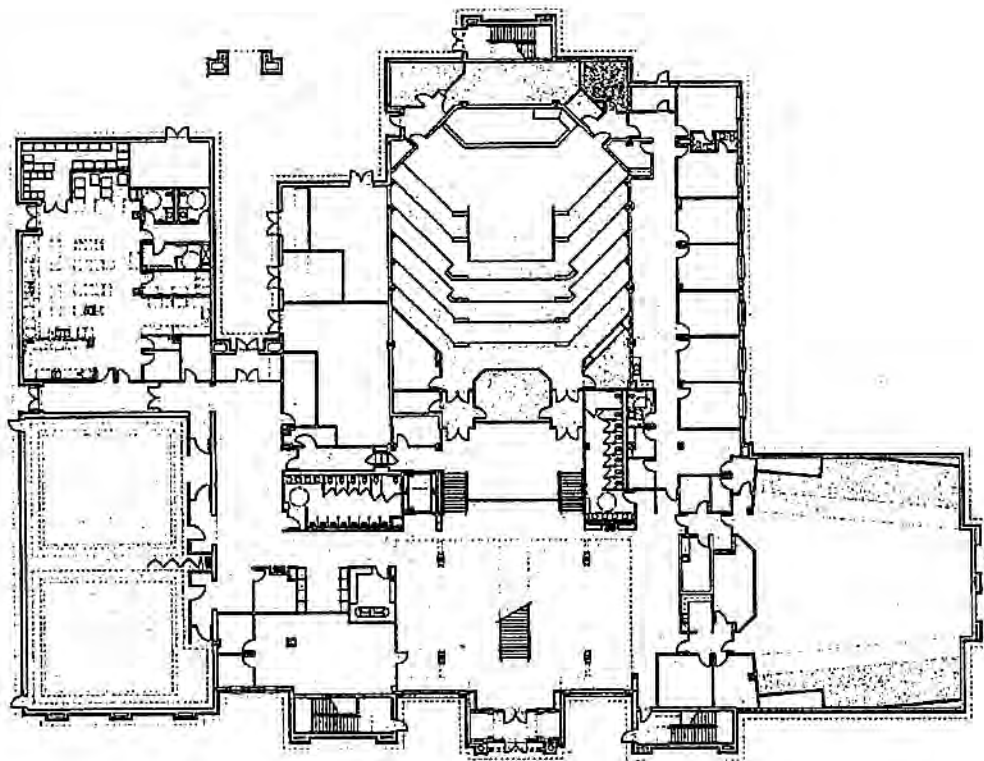
Directions

Driving directions to Smart Center, Andrews AFB, MD

1. I-95 South
2. Take Exit 9 toward Allentown Road/Andrews AFB
3. Merge onto MD-337 W/Forestville Road
4. Turn right onto Allentown Road
5. Turn left onto Westover Drive
6. Turn right onto N. Perimeter Road
7. Turn left onto Arkansas Road
8. Smart Faciltiy is located at 1359 Arkansas Road

UNCLASSIFIED FOR OFFICIAL USE ONLY (FOUO)

Map of Smart Center Facility



Food

Catered Working Lunch

Restaurants near Joint Base Andrews

House of Lee Restaurant

6401 Maxwell Dr, Suitland-Silver Hill, MD 0.1 mi NW
(301) 899-8252

Checkers Drive-In Restaurant

4827 Allentown Rd, Suitland, MD 0.3 mi NE
(301) 736-4179

McDonald's

4777 Allentown Rd, Morningside, MD 0.7 mi NE
(301) 735-1641

Burger King

Airport: Andrews AFB, Joint Base Andrews Naval Air Facility, MD 0.4 mi SW
Andrews Air Force Base
(301) 736-4864

Popeyes Louisiana Kitchen

4913 Allentown Rd, Suitland, MD 0.4 mi NE
(301) 967-1336

Eastern Carry Out

4807 Allentown Rd, Suitland-Silver Hill, MD 0.4 mi NE
(301) 669-0038

Kwiky Kebab

1685 Brookley Ave, Joint Base Andrews Naval Air Facility, MD 0.5 mi E
Andrews Air Force Base
(301) 568-7007

Jiffy Shoppes Restaurants

4773 Allentown Rd, Suitland, MD 0.7 mi NE
(301) 420-8200

Charley's Grilled Subs

1811 G St, Joint Base Andrews Naval Air Facility, MD 0.7 mi E
Andrews Air Force Base
(301) 568-0180



Cyber Wargame 13

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b

(b) (6)

Classified By:
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



Cyber WarGame 13

Mission

Conduct a table-top event focused on the anticipated 2015/6 global cyber environment where USCYBERCOM/NSA, DISA, other CCMDs, Interagency organizations, Coalition Partners, and Industry collaborate and coordinate with one another in the execution of their respective responsibilities in a scenario that features Phase 0, run-up to a crisis, and hostilities. This wargame will characterize future Command and Control of Joint cyber operations and evaluate apportionment of cyber forces across the global mission to inform the development of resource and operational requirements which will assist the individual Services in meeting the needs of Unified Commanders around the world.

Objectives

- Analyze the planned Cyber Mission Force (CMF) laydown, employment concepts, and C2 constructs and an equivalent expected adversarial cyber battle plan
- Analyze wartime authorities, Rules of Engagement, ITO development and approval processes

Outputs

- Recommendations for Joint Cyber Doctrine development
- Recommendations for future Cyber Mission Force operational C2 and force employment requirements
- Recommended authorities required to effectively conduct wartime cyber operations
- Recommendations on expediting the acquisition of military cyber resources

“Title 10” Wargames



Basic Tenets

- Joint (Strategic to Operational level)
- Cyberspace Driven
- Five-year Wargame Epoch
- Annual Event
- USCYBERCOM's Wargame



Working Seminar and Execution Details



Working Seminar (3-7 June)

- ~100 participants (DOD/IC, Team Cyber, DHS/FBI, DISA, Academia/Research, Labs, Industry, Coalition, Legal/Policy)
- Classification: TS REL FVEY (some sessions UNCLASS; SECRET network)
- Location: Jacob E. Smart Bldg, Joint Base Andrews, MD (Auditorium, 3 breakout rooms)
- IT Support: SMART Center has SIPR/NIPR access, laptops, phones

Execution (19-22 Aug)

- Location: Jacob E. Smart Bldg, Joint Base Andrews, MD
- Classification: TS REL FVEY
- Blue: (USCC, DISA, NORTHCOM, PACOM, STRATCOM, Coalition), CONUS (USCC, Service Comp, National Guard, DISA, DHS, FBI, Industry), OCONUS (USCC, PACOM, Service Comp, DISA, Cross-Component)
- Red: Nation State, Non-Nation State Cells
- DV DAY: Thursday of execution week (conclude by noon)

Working Seminar Focal Points

- Environment: JIE, Cloud Architecture, mobile computing, Closed Networks, etc
- Policy: Legal, Authorities, International
- Operations: Force structure, C2, Weapons, TTPs
- Define for DOD/Coalition, Government/Commercial and Adversary

Alternative Cells

- Cross Component C2 (explore C2 of Air, Land, Sea & Cyber Components)
- Trans-National Threat
- Point of Presence (Reserve component's ability to rapidly identify resource providers)

Future Locations

- War Colleges (rotate by service)
 - Newport, Leavenworth, Quantico, Maxwell, etc...



Cyber Wargame Agenda



Day 1 – 19 August		Day 2 – 20 August	
0800-0900	Registration	0830-0900	Day 2 Overview & Move 2 Introduction
0900-1030	• Welcome & Introduction • CW13 Seminar Overview • Red National Strategic Interests • CMF 2013 Workforce Construct • Move 1 Introduction	0900-1200	Move 2 Team Session
1030-1200	Move 1 Team Session	1200-1300	Lunch
1200-1300	Lunch	1300-1530	Move 2 Team Session (Continued)
1300-1530	Move 1 Team Session (Cont)	1530-1615	Move 2 Outbrief
1530-1615	Move 1 Outbrief	1615-1700	Adjudication Sync
1615-1700	Adjudication Sync	1700-	Adjudication Mtg (as needed)
1700-	Adjudication Mtg (as needed)		



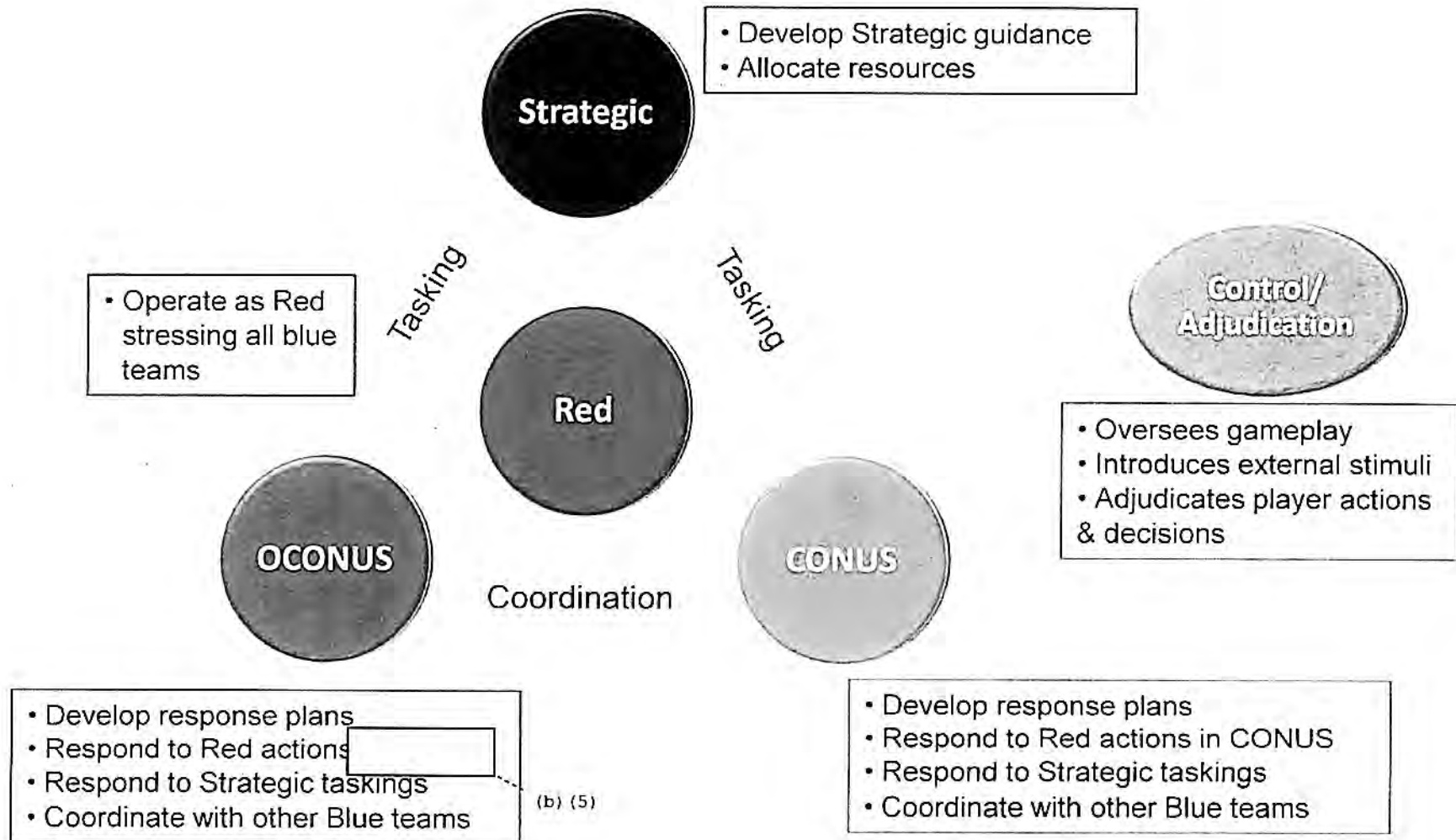
Cyber Wargame Agenda



Day 3 – 21 August		Day 4 (DV Day)– 22 August	
0830-0900	Day 3 Overview & Move 3 Introduction	0800-0930	Senior Leader Hotwash
0900-1200	Move 3 Team Session	0945-1045	Roundtable Discussions
1200-1300	Lunch	1045-1100	Final Closing Remarks
1300-1530	Move 3 Team Session (Continued)		
1530-1615	Move 3 Outbrief and Senior Leader Brief Prep		
1615-1700	Adjudication Sync		
1700-	Adjudication Mtg (as needed)		



Wargame Construct





Teams



Strategic

- Prioritize mission, allocate resources, establish mission tasking
- NSS, OSD, Joint Staff, STRAT, USCC, NORTHCOM, DHS, FBI, Coalition

OCONUS

- Respond to Red actions, determine COAs/LOOs, request resources
- [] JFCCC, [] JFHQ,

CONUS

- Respond to Red actions, determine COAs, request resources
- DHS, FBI, USCC J35, NMF-HQ, NORTHCOM, NGB, Industry

(b) (5)

Red

- Stress Blue teams acting as Red state and unaffiliated transnational actors
- USCC J2, DIA, [] CIA, DIA

Control/ Adjudication

- Introduce injects as required
- Collects data, assess and adjudicates actions by all teams

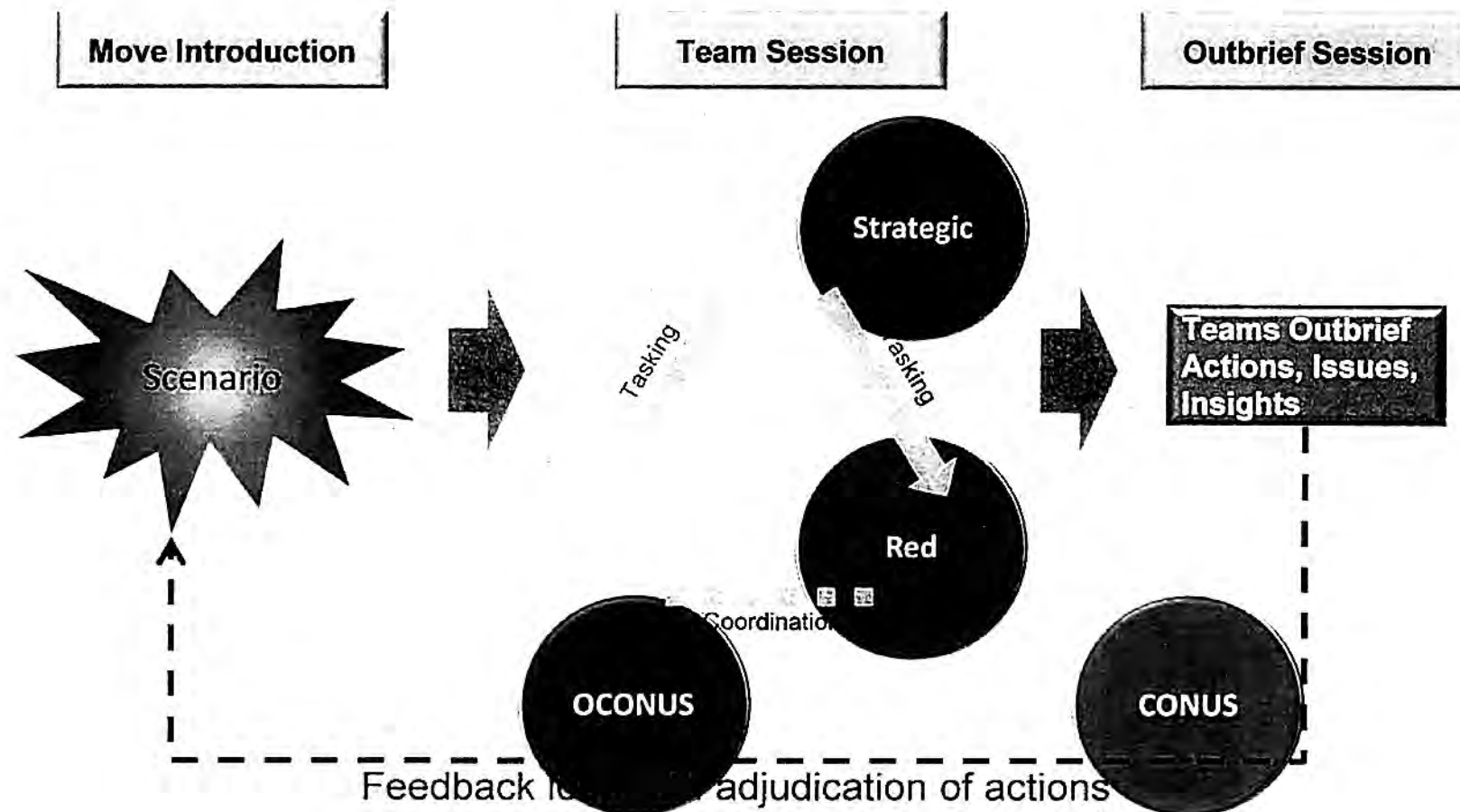


EXERCISE EXERCISE EXERCISE

UNCLASSIFIED//~~FOUO~~



Wargame Methodology



UNCLASSIFIED//~~FOUO~~



Scenario Timeline



CONUS

*Aug 2013 –
Aug 2015*

- DDOS attack on banks
- Vr1x virus discovered on CDC, DODIN, and financial networks
- Reported tests on CIKR systems

*Move 1
Aug 2015*

- Financial sector attacks claimed by transnational actor
- Incidents reported by CIKR
- TRANSCOM impacted

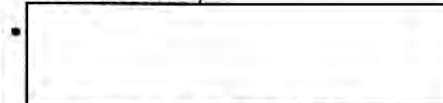
*Move 2
Dec 2016*

- Stock market closes due to attacks
- DDOS attacks reported on ports
- Red conducts attacks on CIKR

*Move 3
Feb 2016*

OCONUS

- Red announces missile test (concern it is cover for attack)



- Increase in exfiltrated US intel/info

(b) (5)

- I&W suggests test is cover for attack
- Reported DODIN intrusions
- POTUS orders execution of FDOs

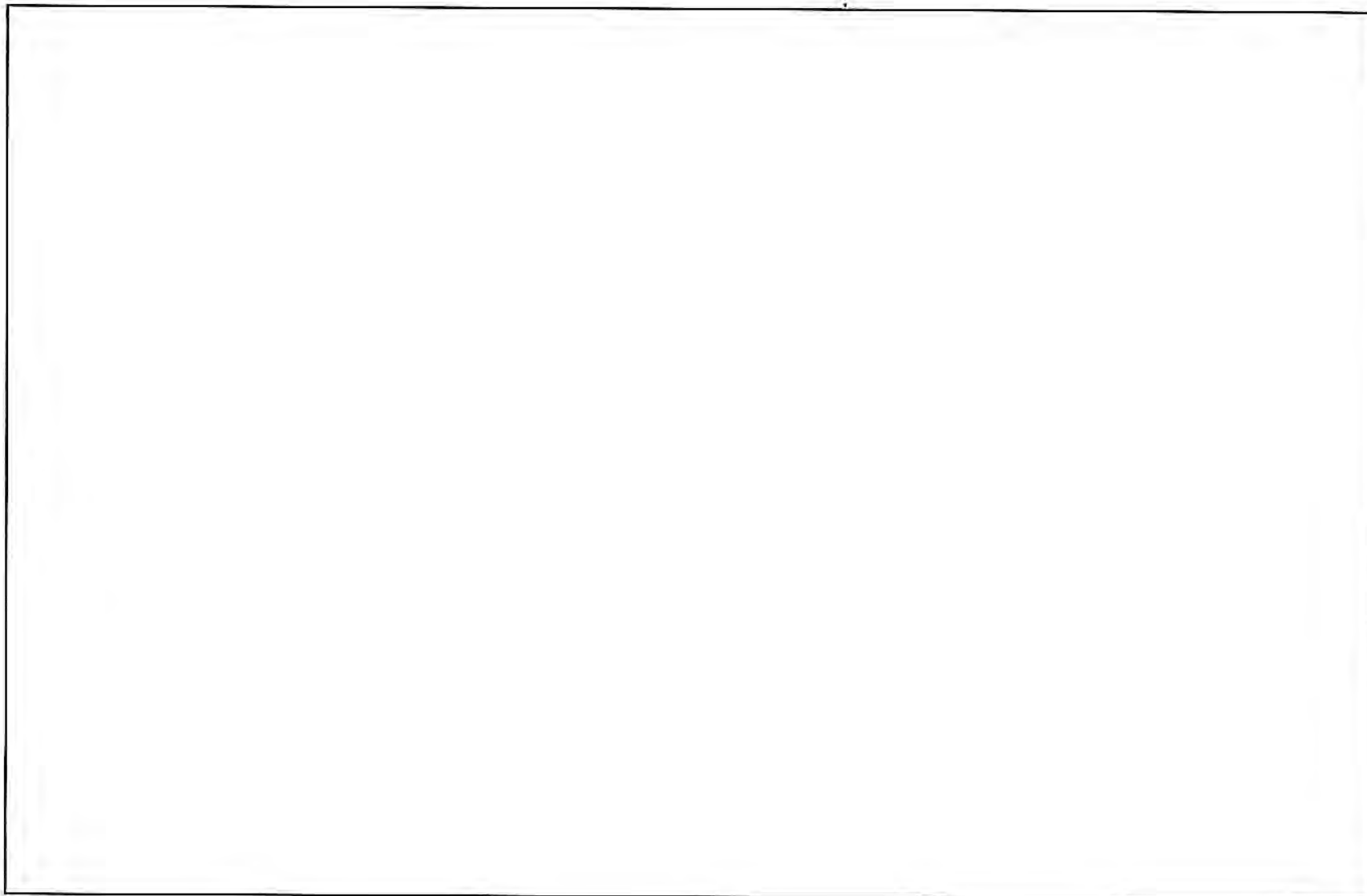
- Red forces do not return to garrison following exercise
- Red begins attack preparations
- Red conducts cyber campaign

Road to Crisis	Phase 0	Phase 1	Phase 2
----------------	---------	---------	---------



Threat Tier Actors

(b) (1) Sec. 1.4 (a)





Joint Cyber Forces

(b) (1) Sec. 1.4(a)

SECRET//REL FVEY



SECRET//REL FVEY



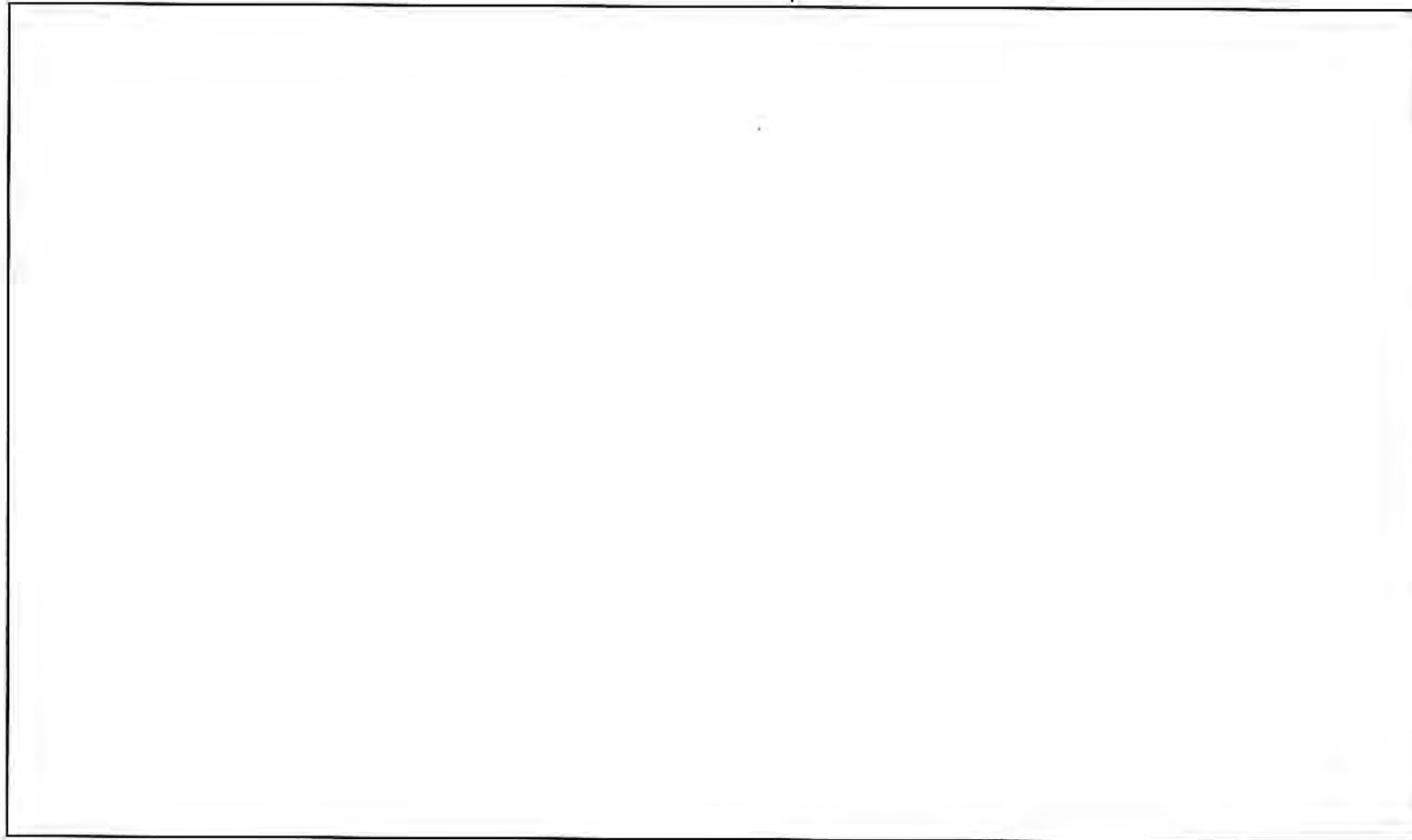
Road to Crisis and Cyber Environment Overview



Road to Crisis

(b) (5)

UNCLASSIFIED//~~FOUO~~

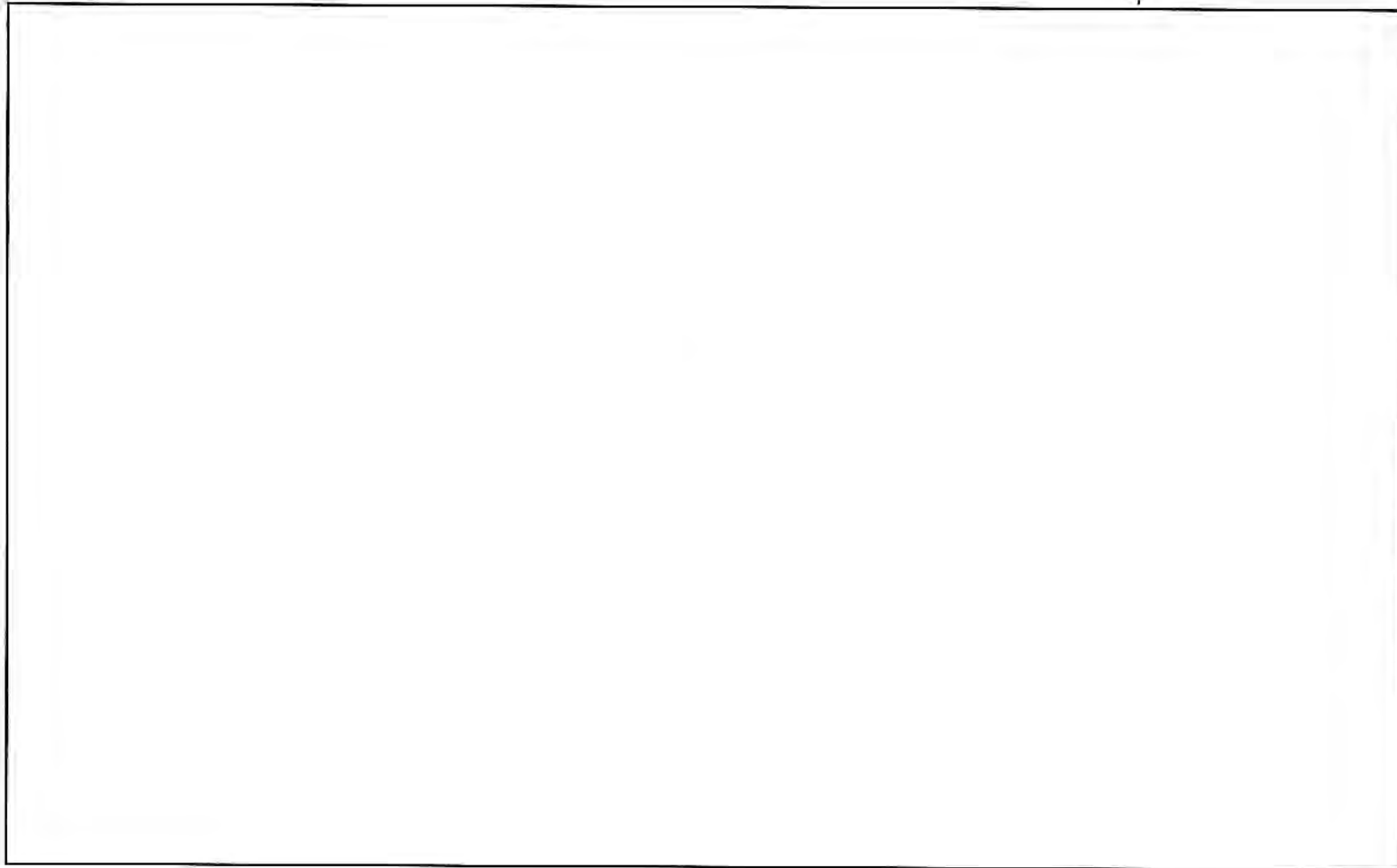


UNCLASSIFIED//~~FOUO~~



Road to Crisis (Continued)

(b) (5)





2013-2015 Cyber Environment

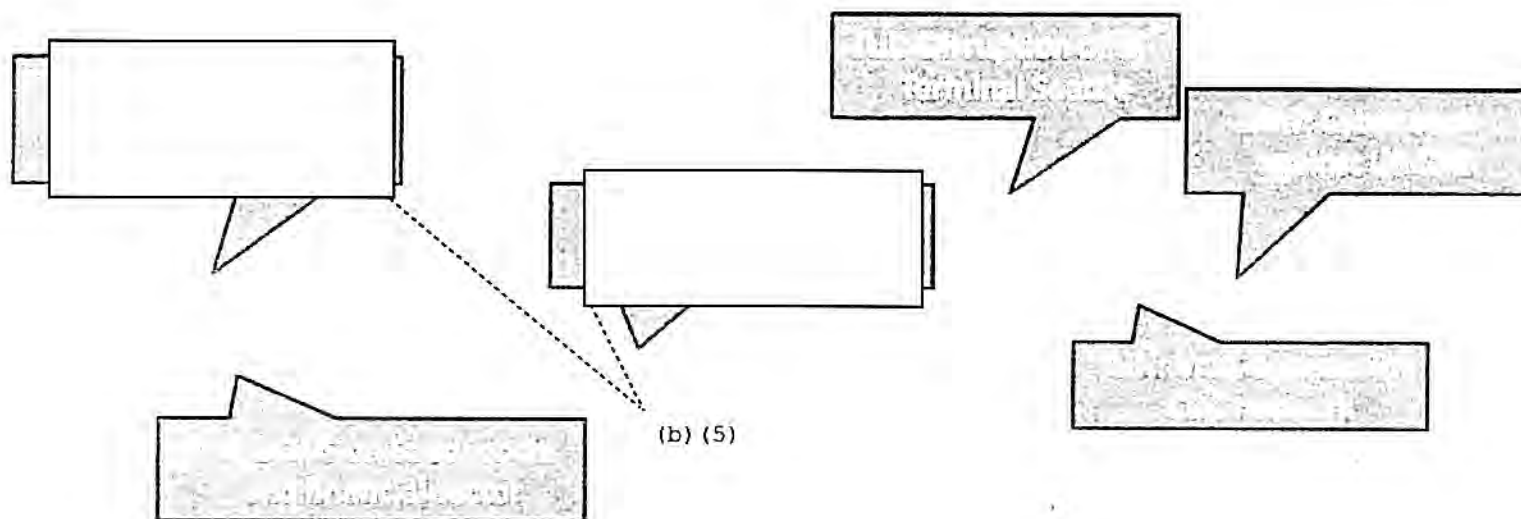


- The quantity and quality of malicious cyber actors (both State and non-State) continues to grow
 - More nations have built cyber capabilities without established norms of behavior
 - Non-state actors not responding to traditional deterrence actions (legal/military)
 - Malicious actors operating with greater frequency without regard for geographic boundaries
- Convergence of technologies has led to greater cyber dependency
 - Military and civilian systems have continued to become more interconnected
 - More vulnerabilities and gateways have developed through systems that were not previously linked
- Critical infrastructure is regularly targeted by both State and non-State actors
 - Financial sector regularly attacked and exploited by cyber actors





Cyber Activities Overview 2015



CONUS

- Intelligence assessments note increasing activity and effectiveness of transnational cyber actors with no apparent linkages to state actors
- Several transnational cyber organizations are increasing cyber infiltration efforts against commercial, federal, and DoD networks
- The sophisticated "Vr1X" appears in CDC networks and has spread throughout industry
- Cyber tests against US CIKR reported

OCONUS

- Red exfiltration of Blue [redacted]
- Unattributed attacks ag [redacted]
- Reports of [redacted]

(b) (5)



Move 1 Scenario



Mid-2015

- June: Tensions between Red and [redacted] increase substantially
 - [redacted]
 - [redacted]
 - Intelligence reports indicate increase in Red's missile capabilities with the goal of [redacted] (b) (5)
- Late-July: The Vr1x virus [redacted]
 - The virus is continuing to effect CDC cloud networks and has begun to impact the financial sector
- August: Red announces it will be conducting a January missile and maritime exercise
 - Significant but unidentified activity reported at Red strategic missile, C2, and space facilities
 - [redacted] increases its security posture in response to Red's announcement



Today is 19 August 2015



- Unattributed cyber actors began a sustained DDOS attack on the nation's top 4 banks this morning
 - Most customers are unable to access bank websites
 - Some customers also reporting inaccuracies with their accounts
- Vr1x continues to impact DOD, CDC, and financial sector networks
 - Virus has been in commercial networks for months and has been modified over time
 - Clear indications the virus was developed by a sophisticated but still unknown actor
- DHS is receiving several reports from CIKR IS managers indicating their networks are being tested
 - Focus appears to be on port and electrical infrastructure



Today is 19 August 2015 (Cont)

- Reports indicate Red may be using the exercises as a preparatory test or cover for an attack
 - Reported uptick in Red cyber operations focused on military and critical infrastructure

- [REDACTED]

- Increase reported in amount of US information targeted for exfiltration

- Focus is on [REDACTED]
- [REDACTED]
- 500MB exfiltrated in the last 24 hours
- Also targeting [REDACTED]

(b) (5)



Taskings



- Strategic Team
 - Develop/Finalize priorities for cyber actions
 - Identify guidance, LOO, deterrence options, senior government response, strategic comms, authorities, and coordination required to manage each priority
 - Address any requests for forces and authorities
- CONUS and OCONUS Teams
 - Set priorities
 - ID Key Cyber Terrain
 - Allocate Resources
 - Gain Authorization (Legal/Policy)
 - Communicate as necessary (Interagency, DOD, Coalition, and Industry)

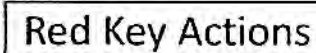
(b) (1) Sec. 1.4 (a)

~~SECRET//REL TO USA, FVEY~~



Cyber Force Requirements

~~SECRET//REL TO USA, FVEY~~



OCONUS Key Actions

CONUS Key Actions



USCYBERCOM CYBER WARGAME 13

Move 2 Scenario/Player Tasking Brief

(b) (3) 10 U.S.C. §130b
(b) (6)

USCYBERCOM

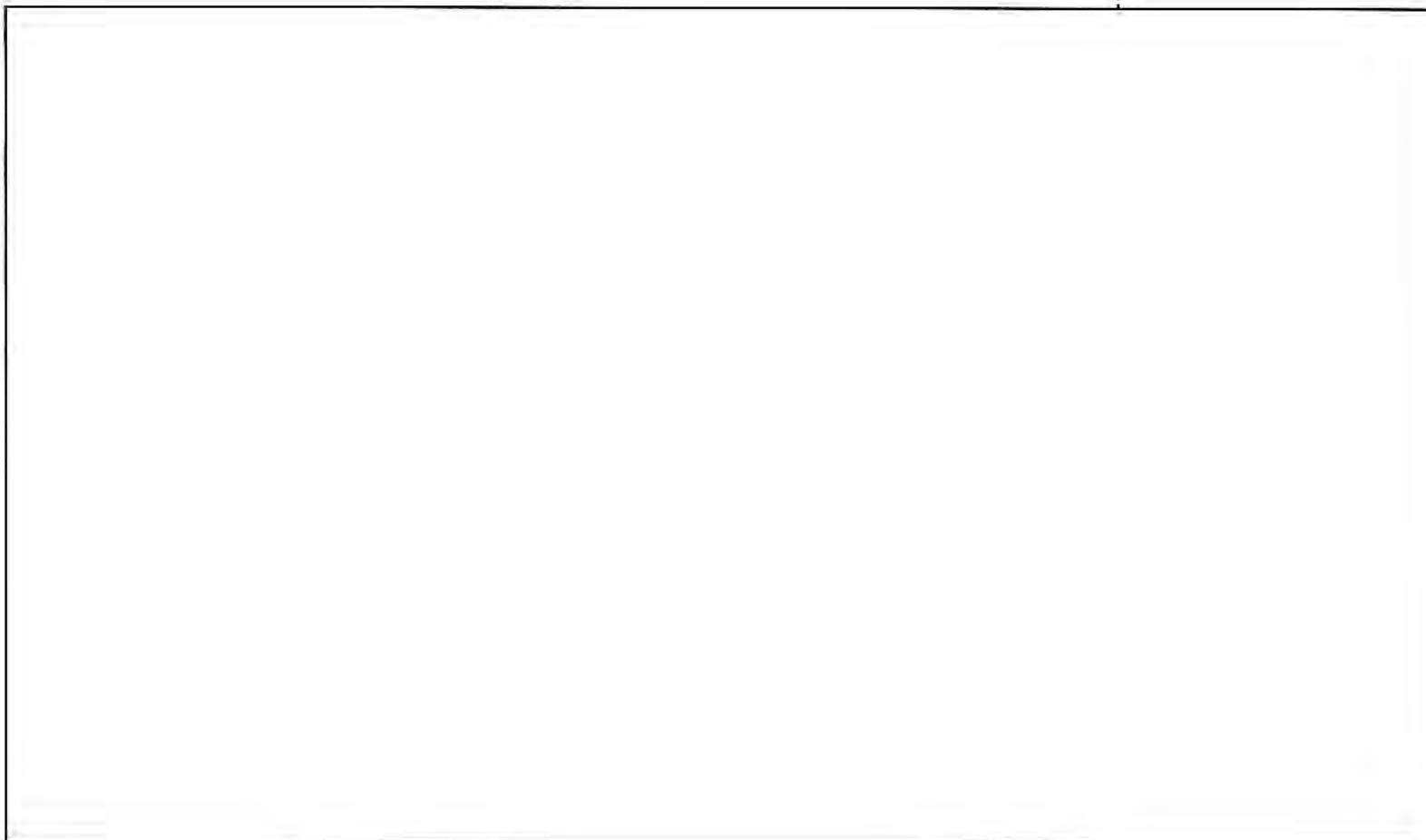
The overall classification of this briefing is: **UNCLASSIFIED//~~FOUO~~**

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



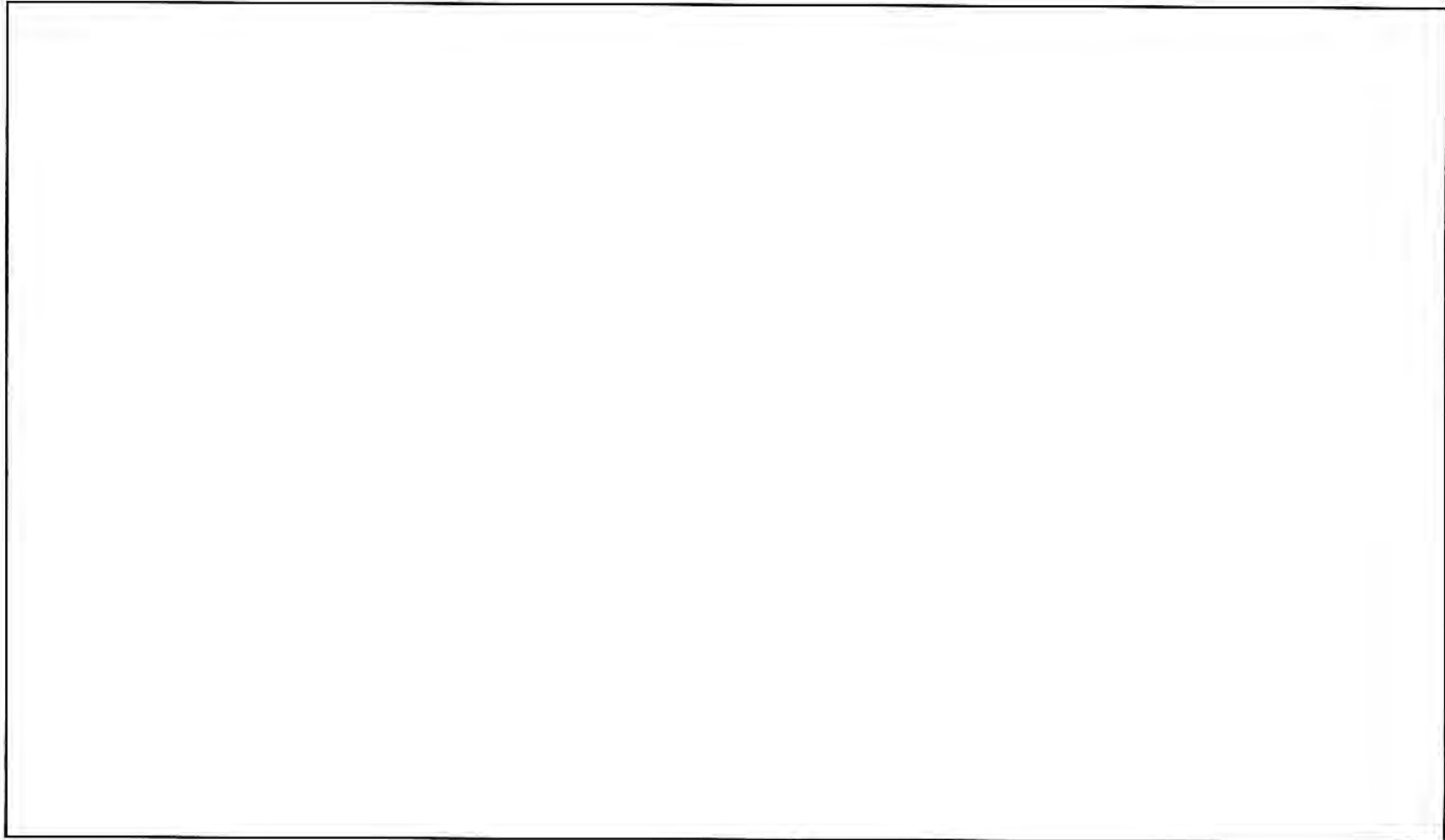
Today is 7 December 2015

(b) (5)





Today is 7 December 2015 (Continued)



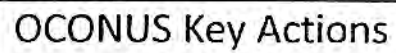
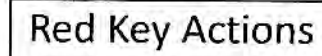
(b) (5)



Taskings



- Strategic Team
 - Develop/Finalize priorities for cyber actions
 - Identify guidance, LOO, deterrence options, senior government response, strategic comms, authorities, and coordination required to manage each priority
 - Address any requests for forces and authorities
- CONUS and OCONUS Teams
 - Set priorities
 - ID Key Cyber Terrain
 - Allocate Resources
 - Gain Authorization (Legal/Policy)
 - Communicate as necessary (Interagency, DOD, Coalition, and Industry)



CONUS Key Actions



USCYBERCOM CYBER WARGAME 13

Move 3 Scenario/Player Tasking Brief

(b) (3) 10 U.S.C. §130b
(b) (6)

USCYBERCOM [REDACTED]

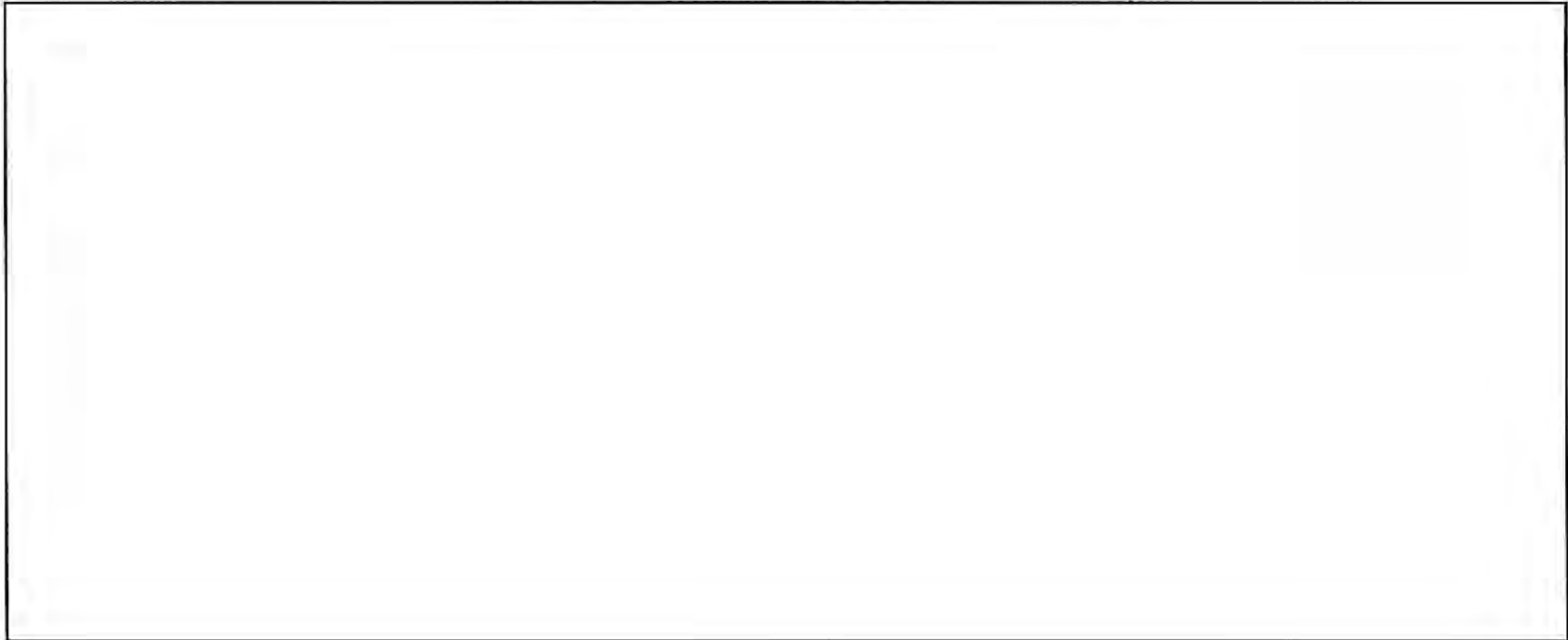
The overall classification of this briefing is: **UNCLASSIFIED//FOUO**

Classified By: [REDACTED]
Derived From: USCYBERCOM/SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



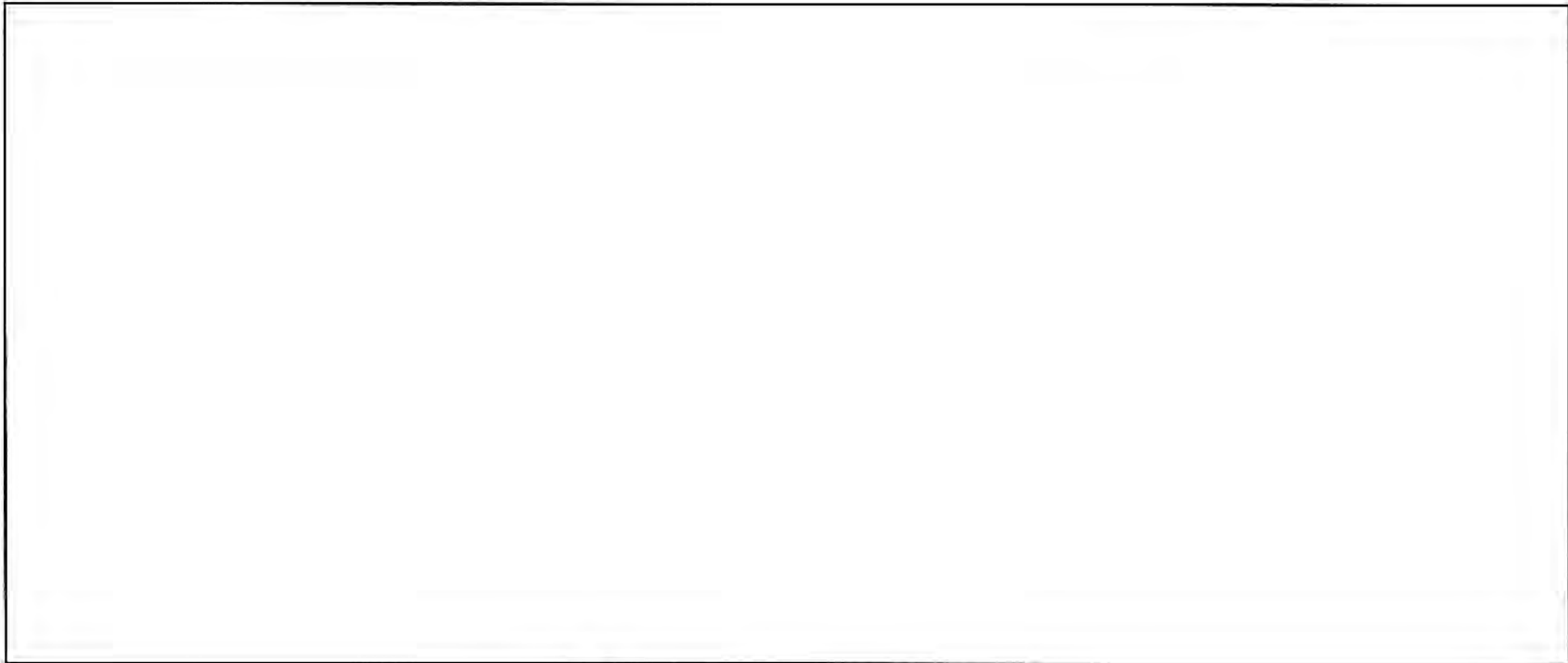
Today is 2 February 2016

(b) (5)





Today is 2 February 2016 (Continued)



(b) (5)

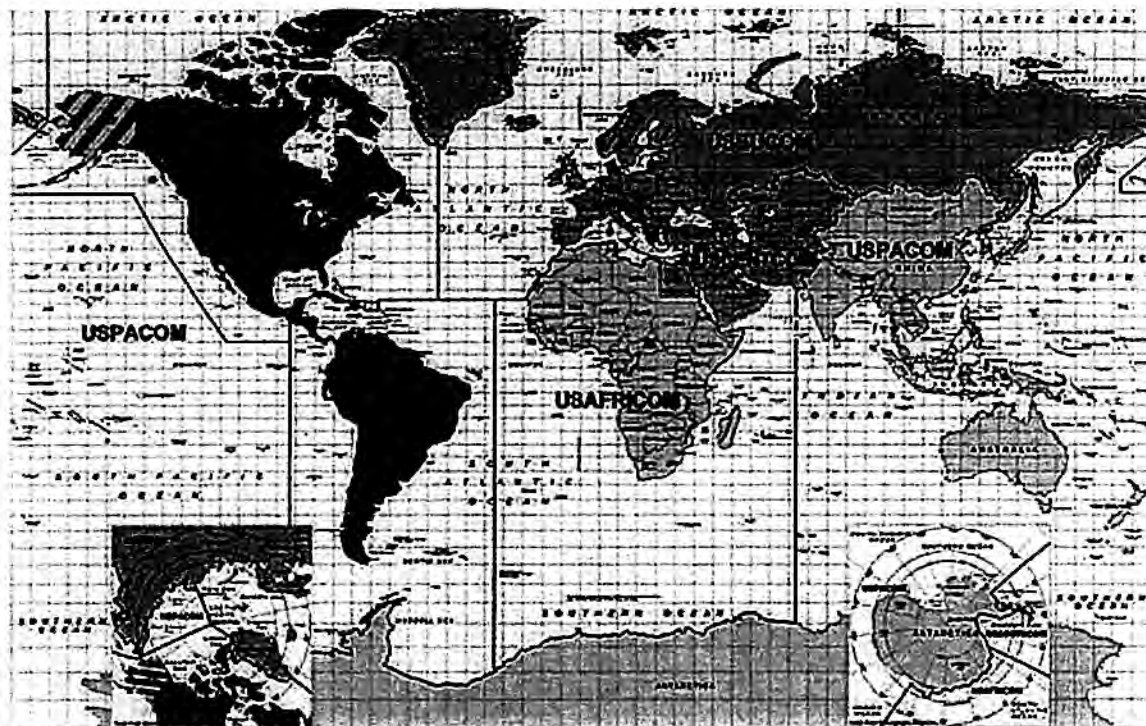


Taskings

- Strategic Team
 - Develop/Finalize priorities for cyber actions
 - Identify guidance, LOO, deterrence options, senior government response, strategic comms, authorities, and coordination required to manage each priority
 - Address any requests for forces and authorities
- CONUS and OCONUS Teams
 - Set priorities
 - ID Key Cyber Terrain
 - Allocate Resources
 - Gain Authorization (Legal/Policy)
 - Communicate as necessary (Interagency, DOD, Coalition, and Industry)



Move 3 Adjudication



Red Key Actions

OCNUS Key Actions

CONUS Key Actions



Mission Slides

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203

Mission Statement

CONUS: National Directives

Mission: In accordance with National Directives and Guidelines secure their unclassified networks against potential intrusion or degradation. Work with owners and operators of critical infrastructure and key resources (CIKR) whether private sector, state or municipality-owned, to bolster their cyber security preparedness, risk assessment and mitigation and incident response capabilities. In the event of cyber incidents against CIKR, the team will coordinate a Federal/State/Local and Industry response to defend, mitigate and remediate impacts to the nation and ensure the continuity of service and the public safety and wellbeing of US persons. Specifically, in accordance with [REDACTED]

[REDACTED]



Capture Template

Team 1 Strategic

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM/SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



Strategic Cyber Priorities



Issue	Pri.	Guidance	LOO	Deterrence Options/ Sr. Gov't Response/ Strategic Comms	Authorities needed / Authorities Delegated	Coord.
-------	------	----------	-----	---	---	--------

--

(b) (1) Sec. 1.4(a)



Strategic Cyber Priorities (Cont)



Issue	Pri.	Guidance	LOO	Deterrence Options/ Sr. Gov't Response/ Strategic Comms	Authorities needed / Authorities Delegated	Coord

(b) (1) Sec. 1.4 (a)



Team Outbrief Questions



- How did you decide which priorities to allocate resources?
How did you identify your key terrain?
- What coordination was required to gain necessary authorities?
- What were your overall shortfalls/issues and how did you mitigate these?



Capture Template

Team 2 OCONUS

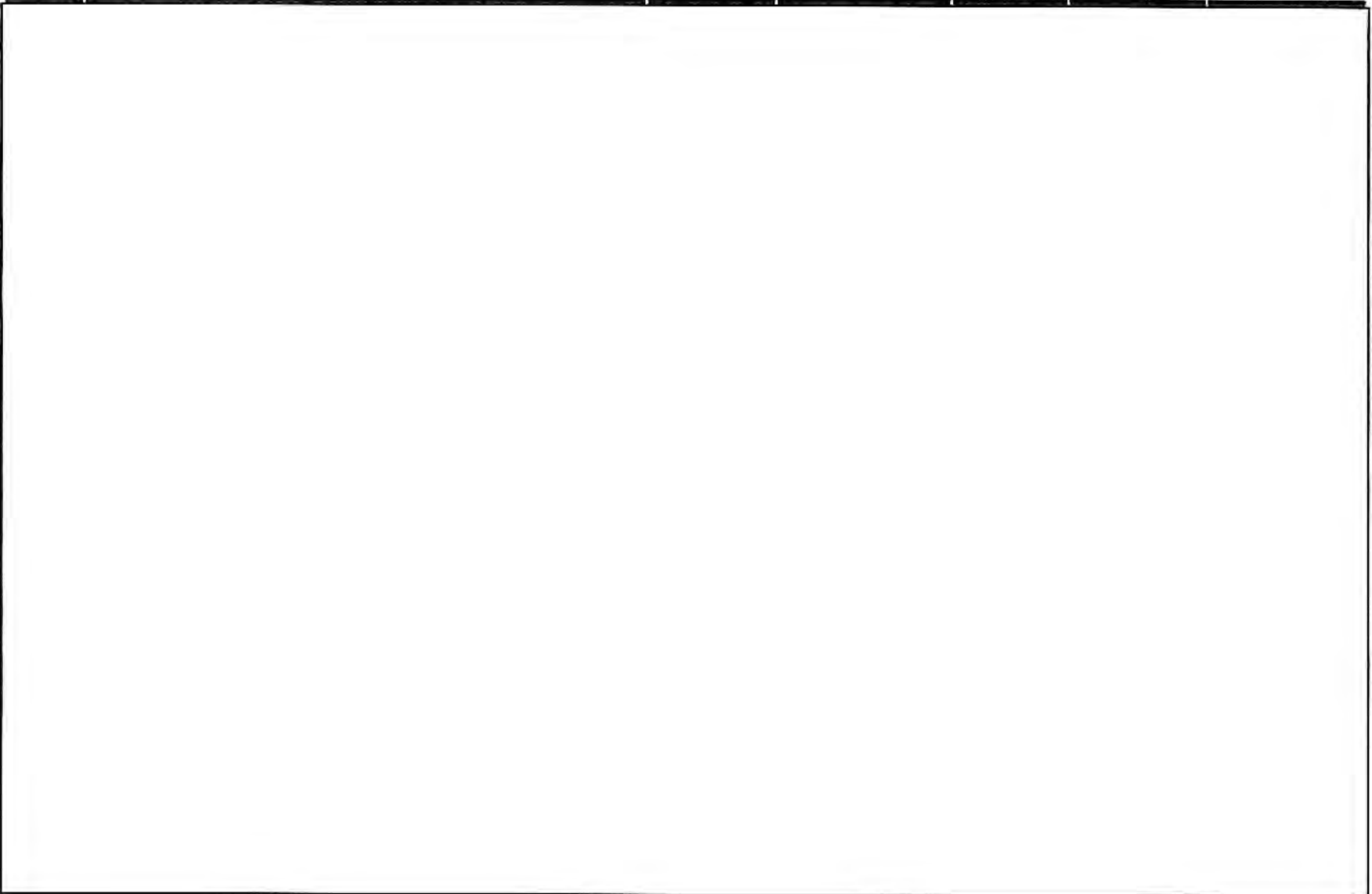
The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By:
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



OCONUS Team Cyber Priorities





Team Outbrief Questions



- How did you decide which priorities to allocate resources?
How did you identify your key terrain?
- What coordination was required to gain necessary authorities?
- What were your overall shortfalls/issues and how did you mitigate these?



Capture Template

Team 3 CONUS

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [REDACTED]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



CONUS Team – Capture Template



Task/ Issue	Sector	Priority	Industry/ Capacity	Response (COA)	Actions Taken	Capabilities/F orces Req'd

(b) (1) Sec. 1.4 (a)



Team Outbrief Questions



- How did you decide which priorities to allocate resources?
How did you identify your key terrain?
- What coordination was required to gain necessary authorities?
- What were your overall shortfalls/issues and how did you mitigate these?



Senior Leader Outbrief Templates

Team 3 CONUS

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

(b) (3) 10 U.S.C. §130b

(b) (6)

Classified By: [REDACTED]

Derived From: USCYBERCOM SCG

Dated: 20111011

AND

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20371203



Strategic Team – AAR



Observation

- 1.
- 2.
- 3.

Solution

- 1.
- 2.
- 3.

Requirements

- 1.
- 2.
- 3.

Next Steps

- 1.
- 2.
- 3.



OCONUS Team – AAR



Observation

- 1.
- 2.
- 3.

Solution

- 1.
- 2.
- 3.

Requirements

- 1.
- 2.
- 3.

Next Steps

- 1.
- 2.
- 3.



CONUS Team – AAR



Observation

- 1.
- 2.
- 3.

Solution

- 1.
- 2.
- 3.

Requirements

- 1.
- 2.
- 3.

Next Steps

- 1.
- 2.
- 3.



Adjudication Template

CONUS

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



Move X Adjudication

Force Allocation Highlights

- Authorized
- Not Authorized
- Implications

PACOM Key Actions

- X
- X
- X

RED Key Actions

- X
- X
- X

CONUS Key Actions

- X
- X
- X



Move X Adjudication – CONUS



CONUS Key Actions

- X
- X
- X

Assessment

- Success
- Shortfalls
- Impacts

Met Mission Objectives: Yes/No

Did force allocation Achieve Desired Results: Yes/No

RED Key Actions

- X
- X
- X



CONUS Team – Issues to Consider Next Move



- Priorities
- Force Assignment/Tasking
- Other



Move X Adjudication – OCONUS



OCONUS Key Actions

- X
- X
- X

Assessment

- Success
- Shortfalls
- Impacts

Met Mission Objectives: Yes/No

Did force allocation Achieve Desired Results: Yes/No

RED Key Actions

- X
- X
- X



OCONUS Team – Issues to Consider Next Move



- Priorities
- Force Assignment/Tasking
- Other



Blue LOOs

CONUS

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SEC
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



CONUS – LOOs



- Title: Industry Led Response
- Description/Actions
 - Individual industries will utilize organic cyber IT and contracted security assets to deter, defend against and respond to enclave specific intrusions.
 - FBI, NCCIC, NSA and USCC will receive specific reporting through USCERT and ISACs based on voluntary industry specific incident reporting in accordance with regulatory policies as required.
 - Federal agencies will facilitate cross-industry reporting in accordance with information sharing policies.
 - US-CERT, NCICC, USCC will facilitate blocks of ISP and patch distribution as required
- Specified Actions
 - On-site remediation (patches, blocks, rerouting)
 - Coordinated Black and White list development
 - Uncoordinated sharing of remediation efforts

Category	Assessment
Resources	Low
Risk/Cost	Low
Success	Moderate
Impact	Moderate
Duration	Short

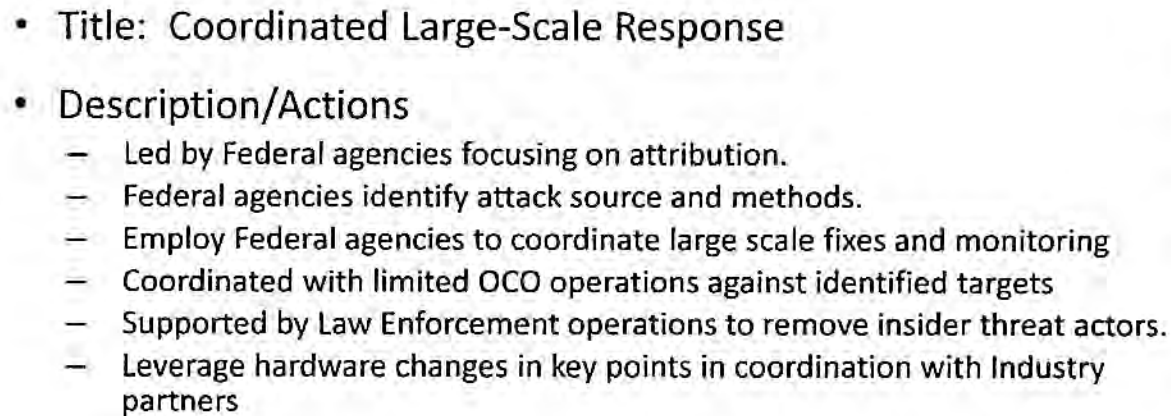


CONUS – LOOs



- Title: State/Federal Incident Response
- Description/Actions
 - State and/or Federal Agencies will direct semi-coordinated response by industry or region
 - State/Federal Assets will deploy to augment/support industry response activities
 - Federal Agencies will more actively support/enable cross-domain solutions (RTAs, Law Enforcement, Information sharing)
- Specified Actions
 - Deployment of State/Federal Incident Response Teams as requested
 - Cross-coordinated development of remediation fixes (patches, IP blocks, TTP sharing)
 - Emphasis on attribution derived from State/Federal Information Collection
 - Redirection of attack sources (IP addresses) to enable point defense hardening
 - Employment of Coordinated firewall deployment (fixes at ISP and Industry security level in coordination with Federal Agencies)
 - Recommendation of dual-use password encryption and best practices. Provide State/Federal assistance if requested.
 - Recommend limiting high bandwidth industry users.
 - Provide funding for augmented and coordinated industry responses.

Category	Assessment
Resources	Medium
Risk/Cost	Low
Success	Moderate
Impact	Moderate
Duration	Moderate



- Specified Actions

Category	Assessment
Resources	High
Risk/Cost	Moderate
Success	High
Impact	High
Duration	High

(b) (1) Sec. 1.4(a)
(b) (3) 10 U.S.C. §130e



CONUS – LOOs



- Title: Unilateral OCO Activities
- Description/Actions
 - Led by Federal agencies focusing on attribution.
 - Federal agencies identify attack source and methods.

Category	Assessment
Resources	Medium
Risk/Cost	High
Success	Medium
Impact	High
Duration	High

- Specified Actions

(b) (1) Sec. 1.4(a)



RED LOOs

CONUS

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM/SCS
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



CONUS – Red LOOs

(b) (1) Sec. 1.4 (a)



Category	Assessment
Resources	Low to High
Risk/Cost	Low to Mod
Success	Mod to High
Impact	Mod to High
Duration	Moderate

Sector and Threat
Actor Specific



CONUS – Red LOOs

(b) (1) Sec. 1.4 (a)



Category	Assessment
Resources	High
Risk/Cost	Moderate
Success	Moderate
Impact	High
Duration	High
Sector and Threat Actor Specific	



CONUS – Red LOOs

(b) (1) Sec. 1.4 (a)



Category	Assessment
Resources	High
Risk/Cost	High
Success	Low
Impact	High
Duration	Medium

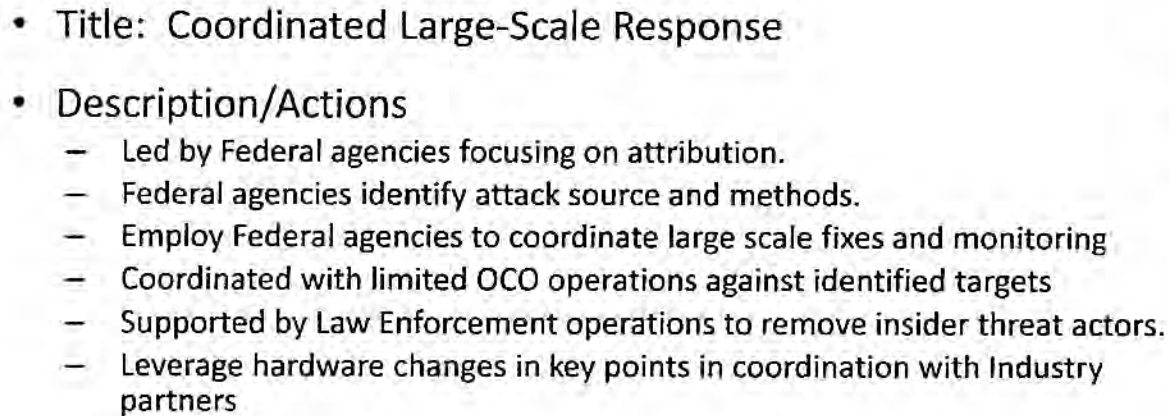


CONUS – LOOs



- Title: State/Federal Incident Response
- Description/Actions
 - State and/or Federal Agencies will direct semi-coordinated response by industry or region
 - State/Federal Assets will deploy to augment/support industry response activities
 - Federal Agencies will more actively support/enable cross-domain solutions (RTAs, Law Enforcement, Information sharing)
- Specified Actions
 - Deployment of State/Federal Incident Response Teams as requested
 - Cross-coordinated development of remediation fixes (patches, IP blocks, TTP sharing)
 - Emphasis on attribution derived from State/Federal Information Collection
 - Redirection of attack sources (IP addresses) to enable point defense hardening
 - Employment of Coordinated firewall deployment (fixes at ISP and Industry security level in coordination with Federal Agencies)
 - Recommendation of dual-use password encryption and best practices. Provide State/Federal assistance if requested.
 - Recommend limiting high bandwidth industry users.
 - Provide funding for augmented and coordinated industry responses.

Category	Assessment
Resources	Medium
Risk/Cost	Low
Success	Moderate
Impact	Moderate
Duration	Moderate



- Specified Actions

Category	Assessment
Resources	High
Risk/Cost	Moderate
Success	High
Impact	High
Duration	High

(b) (3) 10 U.S.C. §130e



CONUS – LOOs



- Title: Unilateral OCO Activities
- Description/Actions
 - Led by Federal agencies focusing on attribution.
 - Federal agencies identify attack source and methods.

- Specified Actions

Category	Assessment
Resources	Medium
Risk/Cost	High
Success	Medium
Impact	High
Duration	High

(b) (1) Sec. 1.4 (a)



RED LOOs

CONUS

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



CONUS – Red LOOs

(b) (1) Sec. 1.4(a)



Category	Assessment
Resources	Low to High
Risk/Cost	Low to Mod
Success	Mod to High
Impact	Mod to High
Duration	Moderate

Sector and Threat
Actor Specific



CONUS – Red LOOs

(b) (1) Sec. 1.4 (a)



Category	Assessment
Resources	High
Risk/Cost	Moderate
Success	Moderate
Impact	High
Duration	High
Sector and Threat Actor Specific	



CONUS – Red LOOs

(b) (1) Sec. 1.4 (a)



Category	Assessment
Resources	High
Risk/Cost	High
Success	Low
Impact	High
Duration	Medium



Facilitator Questions



- What information requirements (PIRs) does the team need addressed to enable their plans and actions?
- What capabilities does the planning rely on in terms of tools, processes and personnel? Are the capabilities currently available or projected for the future timeframe? How are they accounted for? (COTs, enabling, embedded capabilities, etc)
 - What capabilities are not being accounted for in the described force construct?
- What is your perception of the Blue/Red/ROW environment? How does this affect your planning?
- What are your planning constraints (ROE/Auth, resources, etc)? How does this impact planning? What is your mitigation plan?
 - How do plans change with additional authorities?
- Where are you willing to accept risk? Why?
- How can you leverage non-DOD capabilities/resources and authorities from Coalition, Industry, Federal/State, etc)



Facilitator Notes

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



Facilitator Battle Rhythm



- Make players review: Mission, Tasking, Scenario, provided LOOs and Capture Templates
- Players will plan
 - Players will prioritize tasks in accordance with provided mission and LOOs they wish to accomplish
 - Players will modify available LOOs as necessary
 - Players will assign forces
 - Players will provide description details of actions
 - Players will identify shortfalls
- Players will interact
 - Strategic Team will address questions on authorities, force reallocation, National priorities
 - Players will request additional authorities/resources and adjust plan accordingly
 - Red Team/Control will insert injects as appropriate
 - Adjudication will observe team play and prepare for post-move brief.
- Players will complete capture templates and questions
 - Strategic Team: Prioritization slide with provided guidance, authorities, and question slides
 - All other Teams: Prioritization, action description and question slides



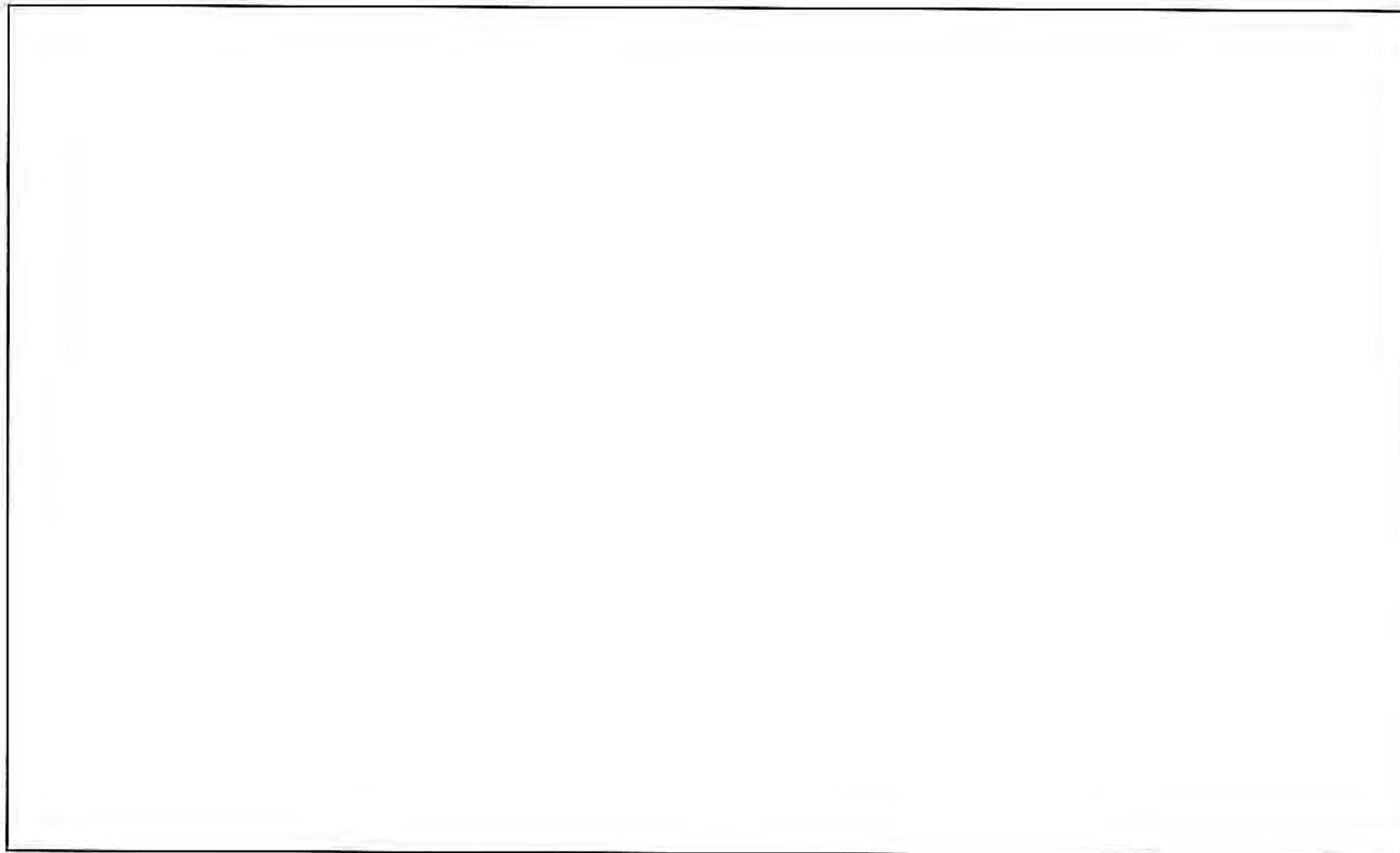
Facilitator Questions



- What information requirements (PIRs) does the team need addressed to enable their plans and actions?
- What capabilities does the planning rely on in terms of tools, processes and personnel? Are the capabilities currently available or projected for the future timeframe? How are they accounted for? (COTs, enabling, embedded capabilities, etc)
 - What capabilities are not being accounted for in the described force construct?
- What is your perception of the Blue/Red/ROW environment? How does this affect your planning?
- What are your planning constraints (ROE/Auth, resources, etc)? How does this impact planning? What is your mitigation plan?
 - How do plans change with additional authorities?
- Where are you willing to accept risk? Why?
- How can you leverage non-DOD capabilities/resources and authorities from Coalition, Industry, Federal/State, etc)



Facilitator Instructions for Force Allocation

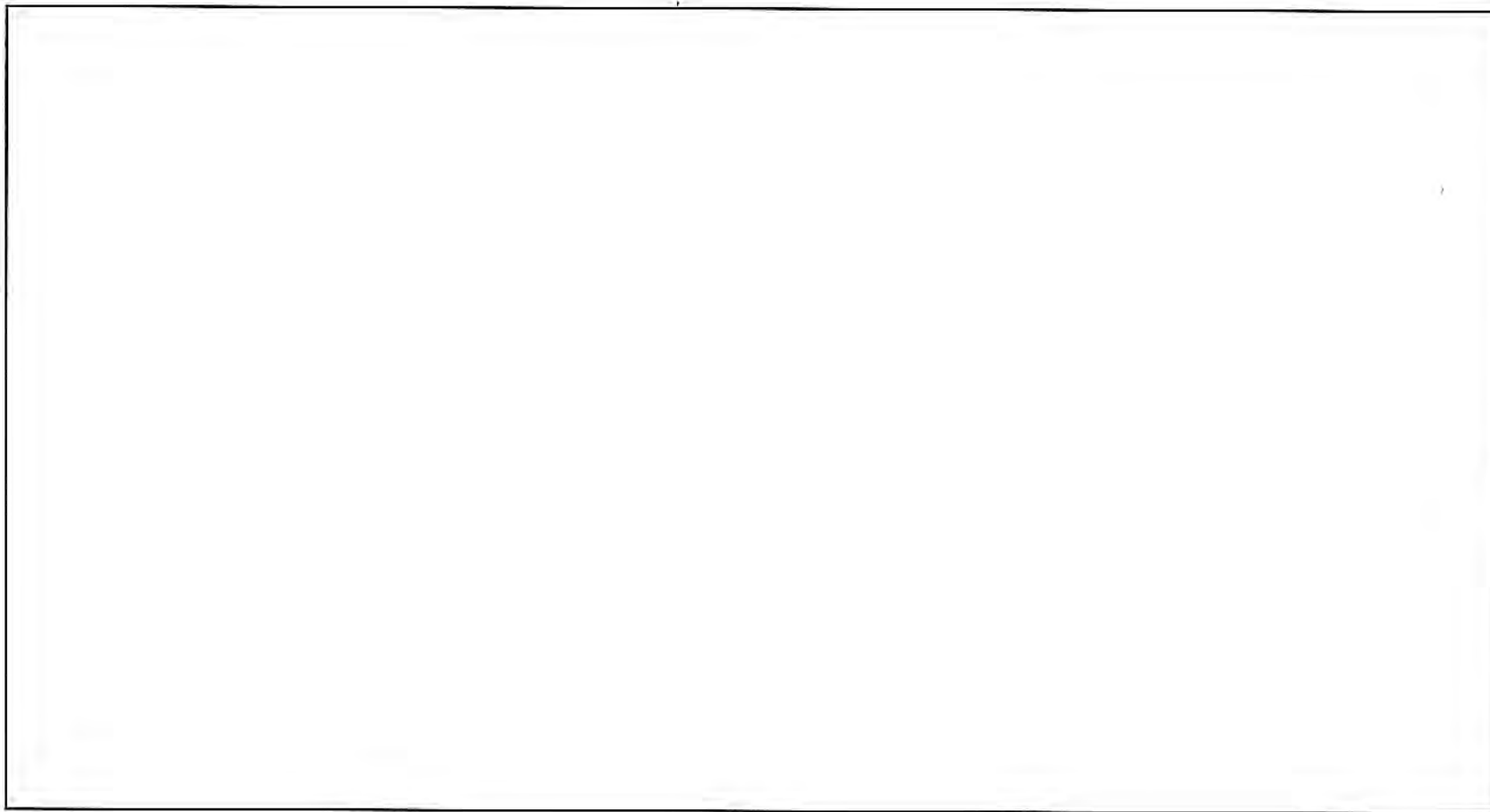


(b) (1) Sec. 1.4 (a)



ROE – Move 1

(b) (1) Sec. 1.4(a)





Cyber Wargame 13

Defining USCYBERCOM 5-year Requirements

USCYBERCOM/J7

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By: [redacted]
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203



Cyber Wargame 13

Mission

Characterize the joint cyber resource and operational requirements through FY2018 in order to assist the Services fulfill their Title 10 responsibilities to organize, train, and equip forces for Unified Commander employment.

Objectives

- Analyze the planned Cyber Mission Force (CMF) laydown, employment concepts, and C2 constructs and an equivalent expected adversarial cyber battle plan
- Analyze wartime authorities, Rules of Engagement, ITO development and approval processes
- Explore future friendly and adversary cyber environments and their impacts on cyber operations
- Identify future policy and coordination constraints in the cyber realm
- Identify cyber tools, capabilities, and their recommended resource providers necessary to conduct cyber operations from ISR through operations to BDA in the future cyber environment

Outputs

- Recommendations for future Cyber Mission Force operational C2 and force structure requirements
- Recommended authorities required to effectively conduct wartime cyber operations
- A recommended list of cyber capabilities, tools, and supporting policies necessary to conduct cyber operations
- Recommendations to more effectively identify requirement solutions
- An assessment of the future cyber environment and an established baseline for Cyber Wargame 14
- Recommended inputs to USCYBERCOM's training exercises (Cyber Flag/Guard/Knight)

(b) (3) 10 U.S.C. §130b

(b) (6)



Attributes

Basic Tenets

- Joint (Strategic to Operational level)
- Cyberspace Driven
- Five-year Wargame Epoch
- Annual Event
- USCYBERCOM's Wargame

Complementary Elements

- Cyber Adversary Tactics Office
- Cyber Knight/Guard/Flag
- Previous Events (Schriever Wargame, OSD-CAPE, Cyber Linx, ...)

Keys to Success

- 5-yr projection fidelity
- Cyber thought leaders as participants for 3 seminars and execution
- Build a model for post-game trade-space fine-tuning

Status

- Experienced team in place
- Scenario development
- Seminar Construct/Cyber expert rolodex
- Preliminary model of Cyber Flag 13-1 built



(b) (3) 10 U.S.C. §130b
(b) (6)



Seminar and Execution Details

Requirements

- ~50-60 participants (Team Cyber, DOD/IC, DHS/FBI, Academia/Research, Labs, Industry, Coalition, Legal/Policy)
- Classification: TS/SCI REL FVEY (SECRET network)
- Location: SMART Center, Andrews AFB (Auditorium, 3 breakout rooms)
- Event Length: ~3 days (1/2-day academics)
- Budget: \$0 (local mil/gov support)
- IT Support: SMART Center has SIPR/NIPR access, laptops, phones

Execution

(b) (1) Sec. 1.4 (a)

- Blue: Team Cyber Ops Centers down to CMF cells, IC, Coalition
- Red: [REDACTED]
- Green: DHS, FBI, Industry, Legal/Policy Cells
- Adjudication: 2 Game Moves/day
- Support
- DV Day: 7 June (conclude by noon)

Seminar Focal Points

- Environment (#1): JIE, Cloud Architecture, mobile computing, Closed Networks, etc
- Policy (#2): Legal, Authorities, International
- Operations (#3): Force structure, C2, Weapons, TTPs
- Define for DOD/Coalition, Government/Commercial and Adversary

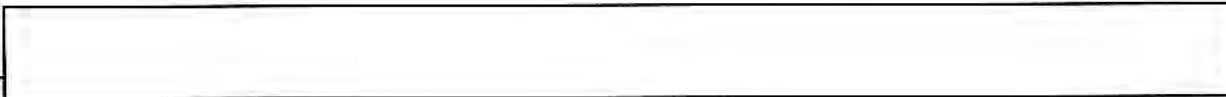
Alternative Cells

- Cross Component C2 (explore C2 of Air & Cyber Components)
- Trans-National Threat
- Point of Presence (Reserve component's ability to rapidly identify resource providers)

(b) (3) 10 U.S.C. §130b
(b) (6)

(b) (1) Sec. 1.4(a)

~~SECRET//REL FVEY~~



~~SECRET//REL FVEY~~

2/19/2013 10:00 VERSION:7



(b) (3) 10 U.S.C. §130b
(b) (6)

5 5



May 2013

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
			1	2	3	4
5	6 Academics	7	8	9	10	11
	CW 13 Seminar #1 – Environment (Joint Base Andrews)					
12	13	14	15	16	17	18
				CW 13 Seminar #2 – Policy (Joint Base Andrews)		
19	20	21	22	23	24	25
	CW 13 Seminar #3 – Operations (Joint Base Andrews)				Down Day	
26	27 HOLIDAY	28	29	30	31	

UNCLASSIFIED//FOR OFFICIAL USE ONLY

2/19/2013 10:00 VERSION:7

(b) (3) 10 U.S.C. §130b
(b) (6)



June 2013

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday
						1
2	3 Academics	4	5	6	7 DV Day	8
	Cyber Wargame 13 (Joint Base Andrews)					
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29

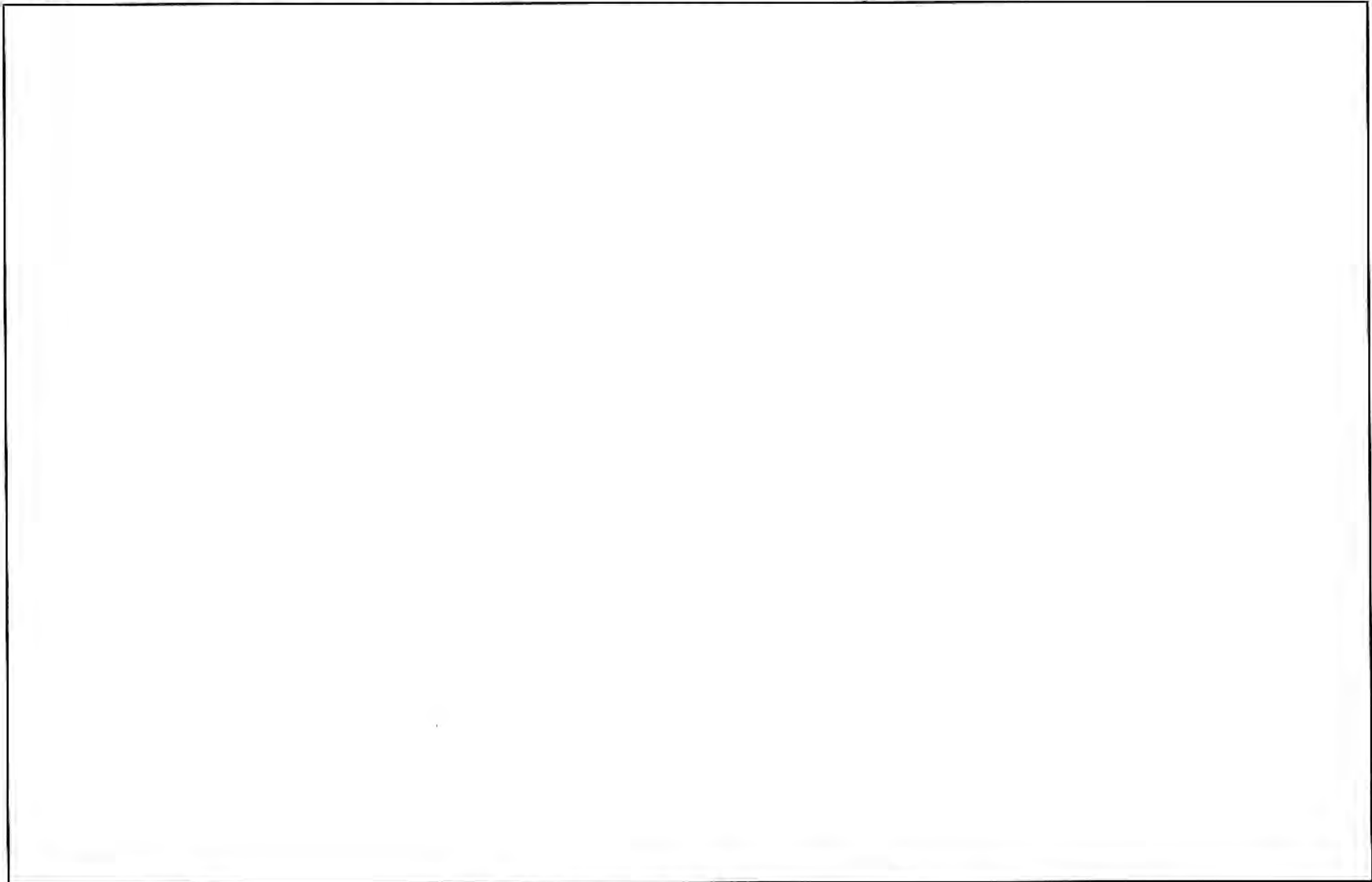
15-16 July

CW 13 AAR/14 CDC
(Joint Base Andrews)



Cyber Wargame Model

(b) (3) 10 U.S.C. §130e





Defining 2018 Cyber Requirements

- 1) What are the most pressing cyber weapon requirements?
- 2) What are the most important operational issues/challenges to shape or prepare the future USCYBERCOM workforce?
- 3) What are the most critical policy requirements?
- 4) Where should USCC/DOD invest resources for the future cyber fight/cyber operations? (people, processes, tools/capabilities)
- 5) Who are the recommended participants for Cyber Wargame 13? (Academia, Labs, Private/Public Sector, Financial Community, DoD/IC...)

(b) (3) 10 U.S.C. §130b
(b) (6)

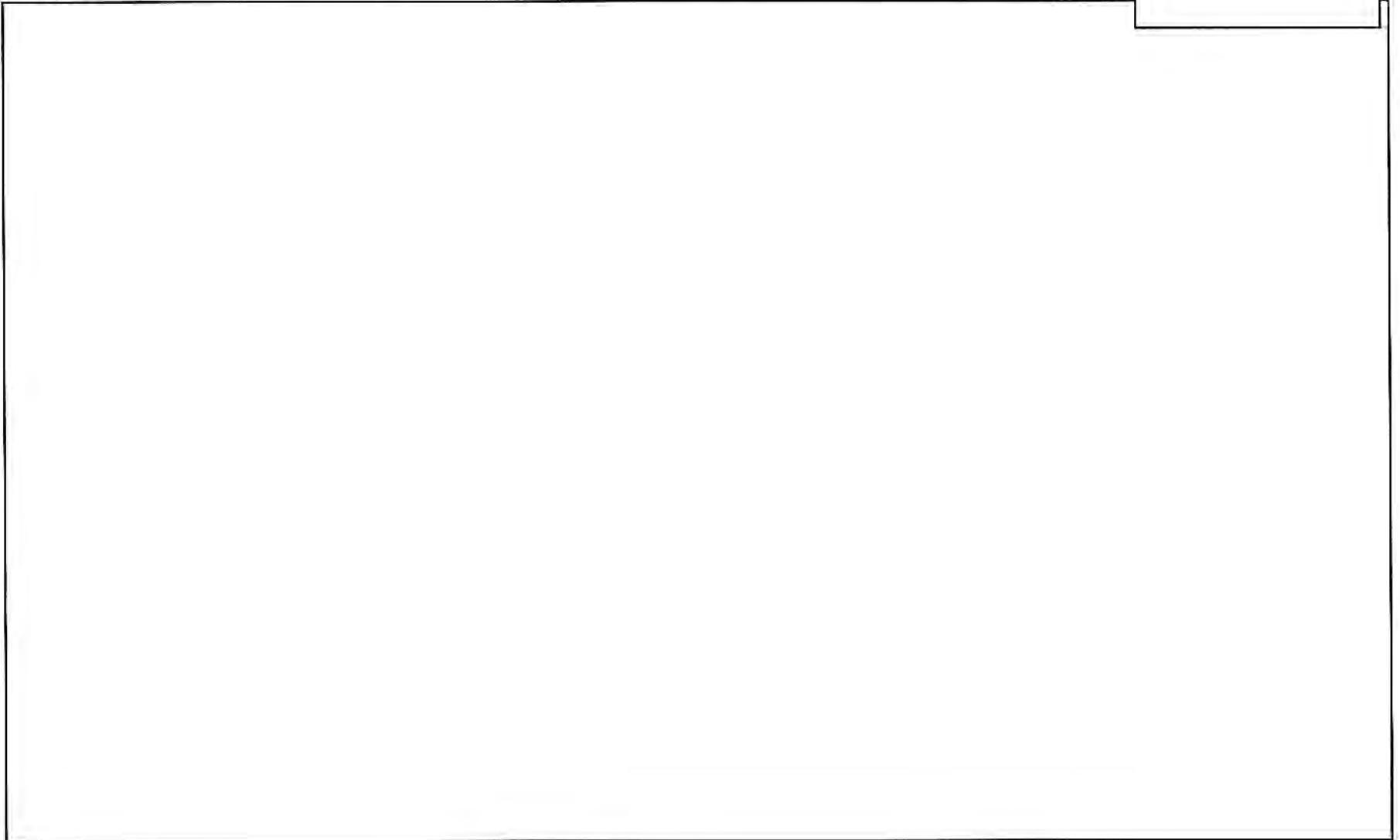


(b) (1) Sec. 1.4 (a)



Cyber Wargame C2 Model – (EOY 2018)

~~SECRET//REL TO USA, FVEY~~



~~SECRET//REL TO USA, FVEY~~

2/19/2013 10:00 VERSION:7

(b) (3) 10 U.S.C. §130b
(b) (6)



Questions

(b) (3) 10 U.S.C. §130b
(b) (6)





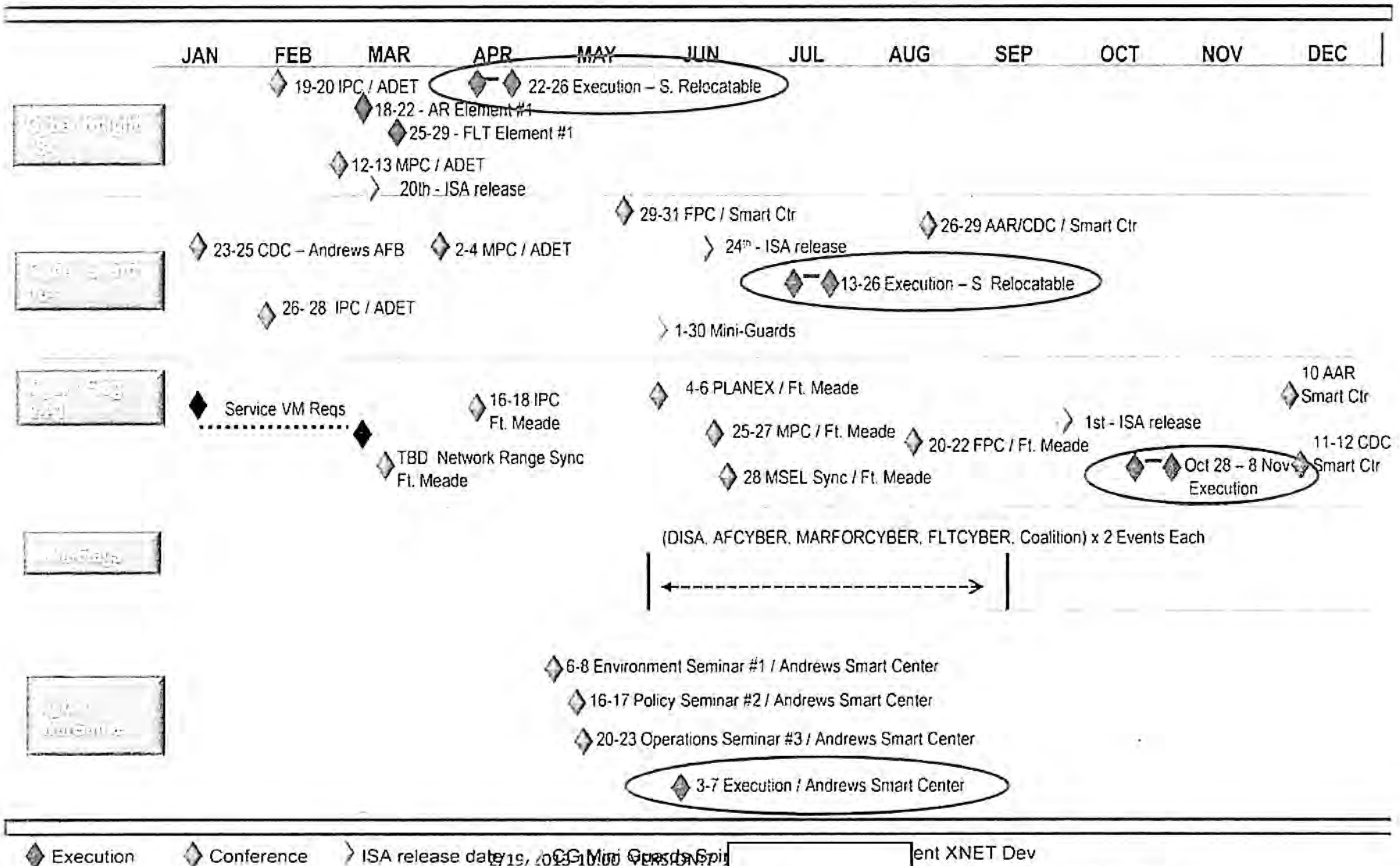
BACKUP SLIDES

(b) (3) 10 U.S.C. §130b
(b) (6)





USCYBERCOM 2013 Exercise and Wargame Plan





Joint Cyber Forces 2018

(b) (1) Sec. 1.4 (a)

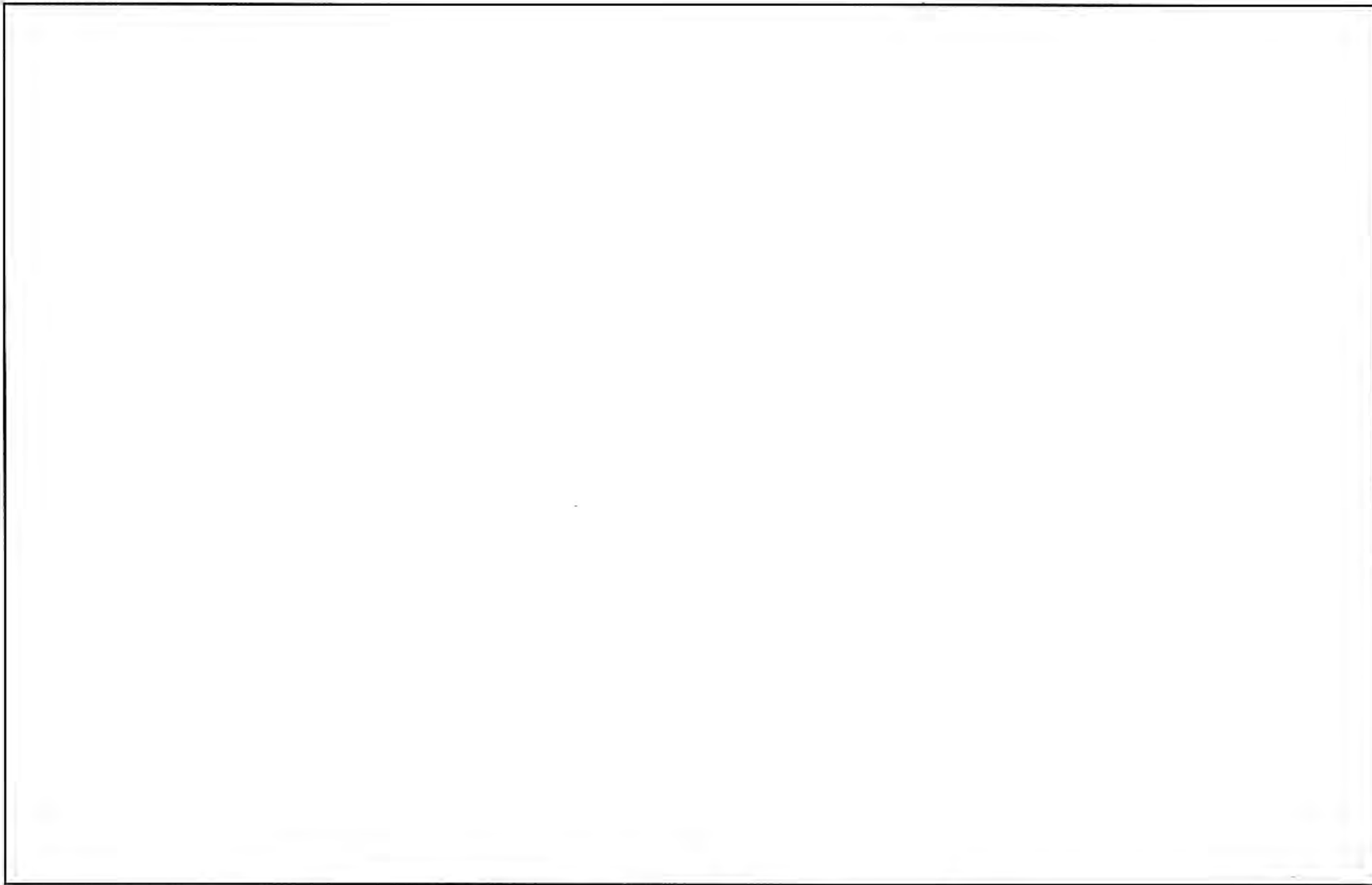
...



(b) (1) Sec. 1.4 (a)
(b) (5)



World Situation 2018 – Geo-political Trends



2/19/2013 10:00 VERSION:7

(b) (3) 10 U.S.C. §130b
(b) (6)



World Situation – 2018

(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET/REL FVEY~~

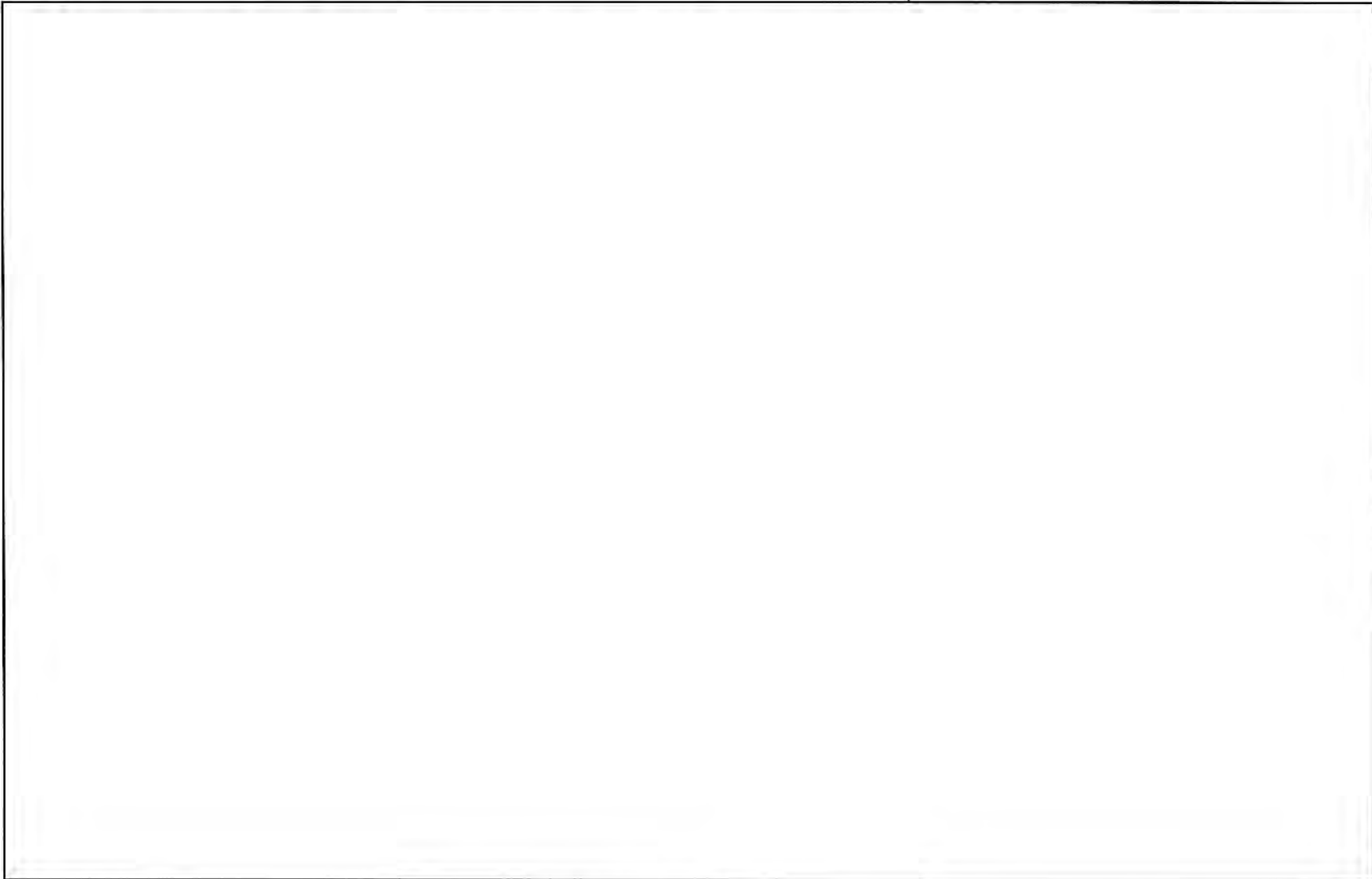
~~SECRET/REL FVEY~~

2/19/2013 10:00 VERSION:7

(b) (3) 10 U.S.C. §130b
(b) (6)



World Situation 2018 – Cyber Trends

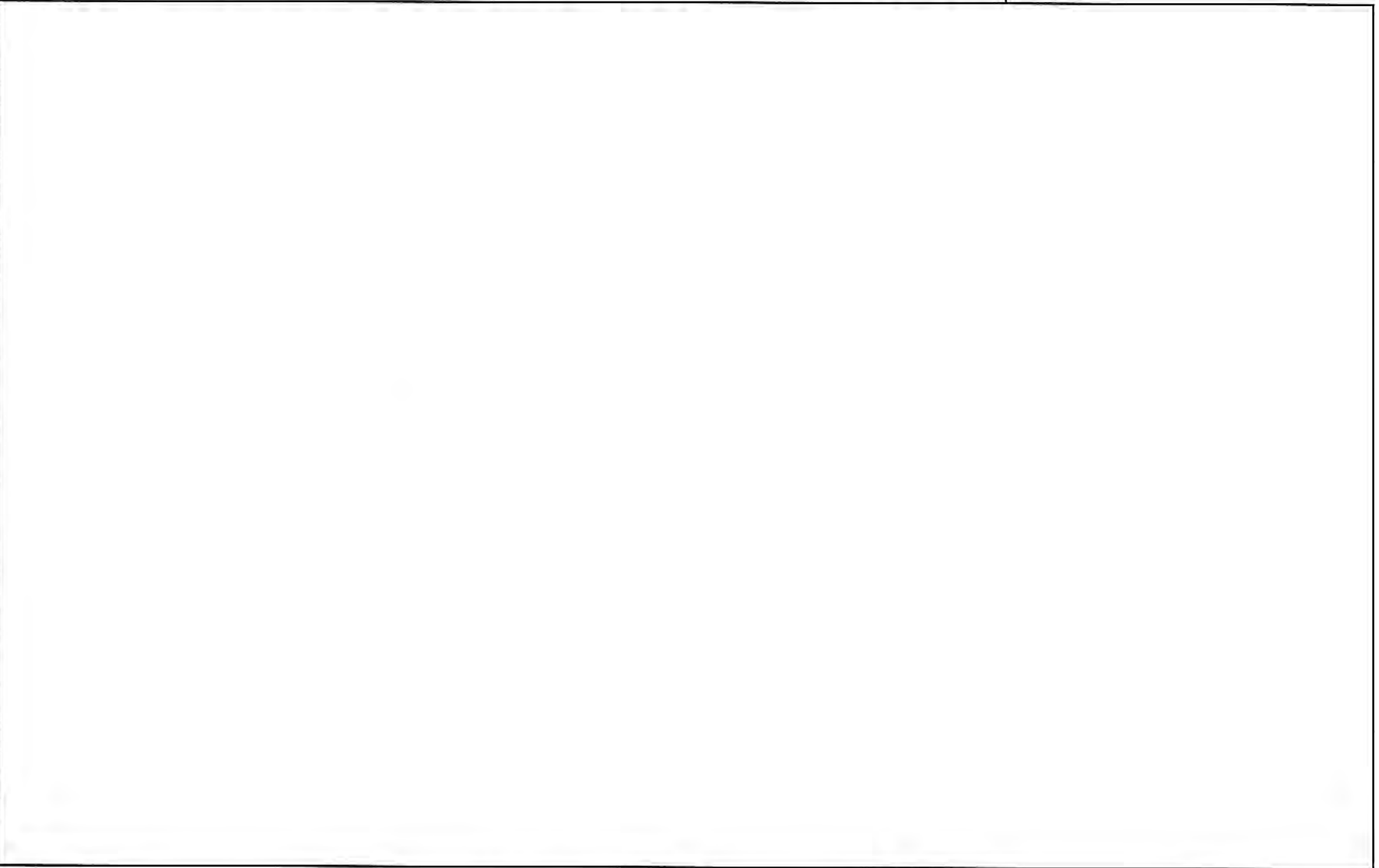


(b) (1) Sec. 1.4(a)
(b) (5)

~~SECRET/REL FVEY~~



World Situation Cyber – 2018



~~SECRET/REL FVEY~~

2/19/2013 10:00 VERSION:7



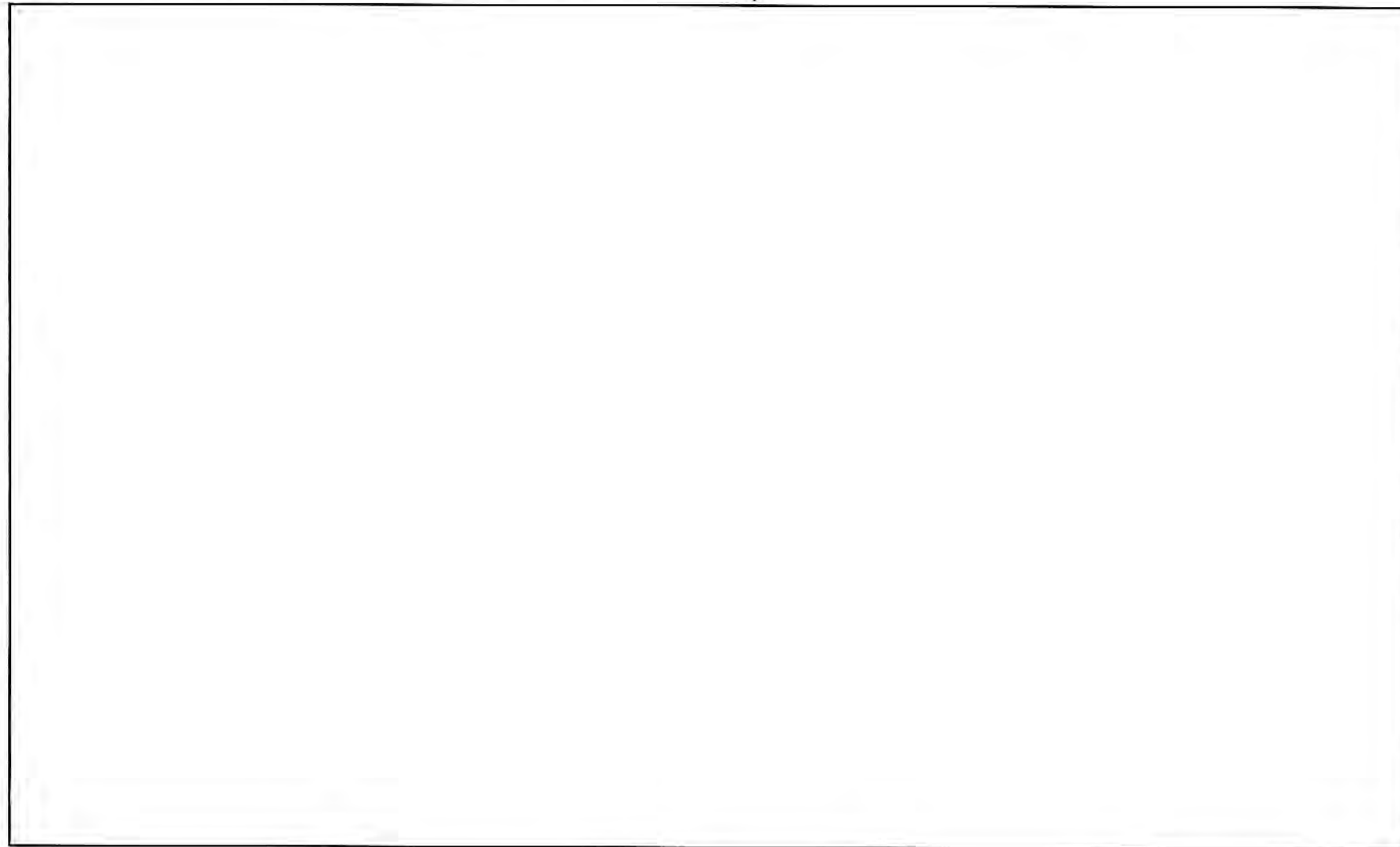
(b) (3) 10 U.S.C. §130b
(b) (6)



Seminar Vignettes

(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET/REL FVEY~~



~~SECRET/REL FVEY~~

2/19/2013 10:00 VERSION:7



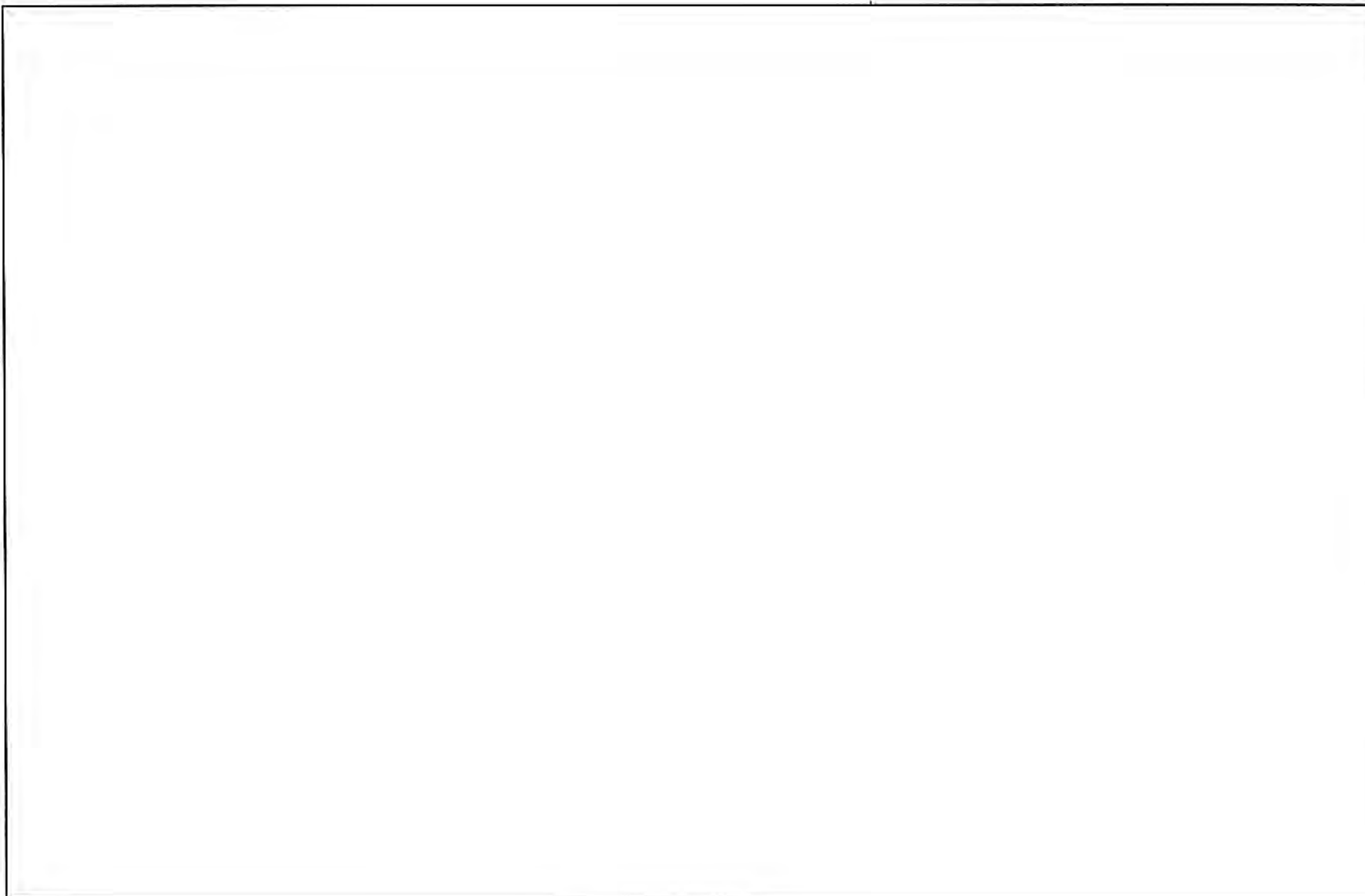
(b) (3) 10 U.S.C. §130b
(b) (6)



Wargame Vignettes

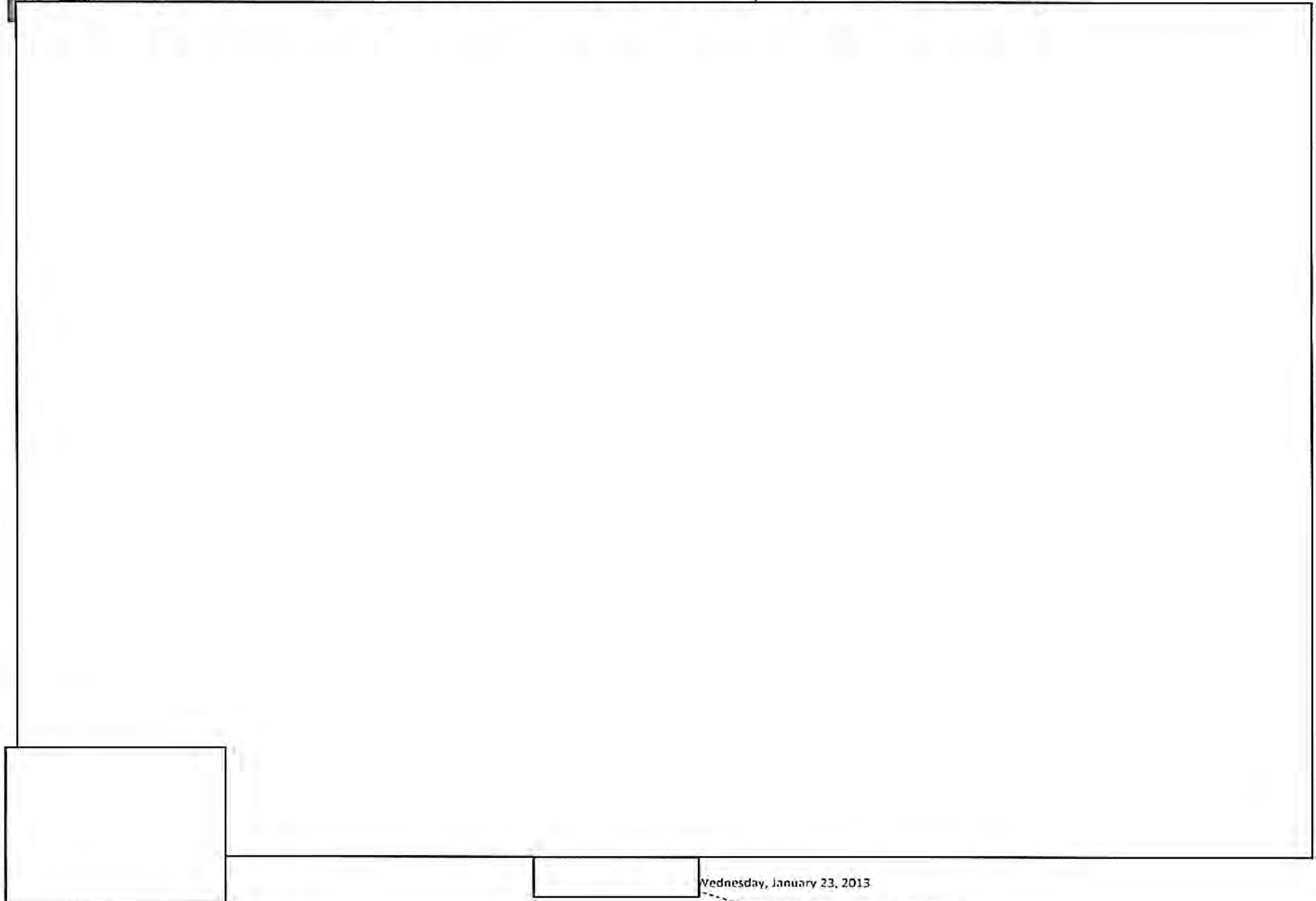
(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET/REL FIVE~~





Cyber Wargame C2 Model – (EOY 2018)



Wednesday, January 23, 2013

(b) (3) 10 U.S.C. §130b
(b) (6)



Cyber Flag 13-1

Performance Summary

(b) (1) Sec. 1.4 (a)
(b) (5)

SECRET//REL FVEY



--



Cyber Wargame 13

Cyber Ops Assessment Framework

MOVE 3

The overall classification of this briefing is: ~~SECRET//REL FVEY~~

(b) (3) 10 U.S.C. §130b
(b) (6)

Classified By:
Derived From: USCYBERCOM SCG
Dated: 20111011
AND
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20371203

FOR WARGAME PURPOSES ONLY

(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET//NOFORN~~



OCO & DCO-RA Operational Assessment

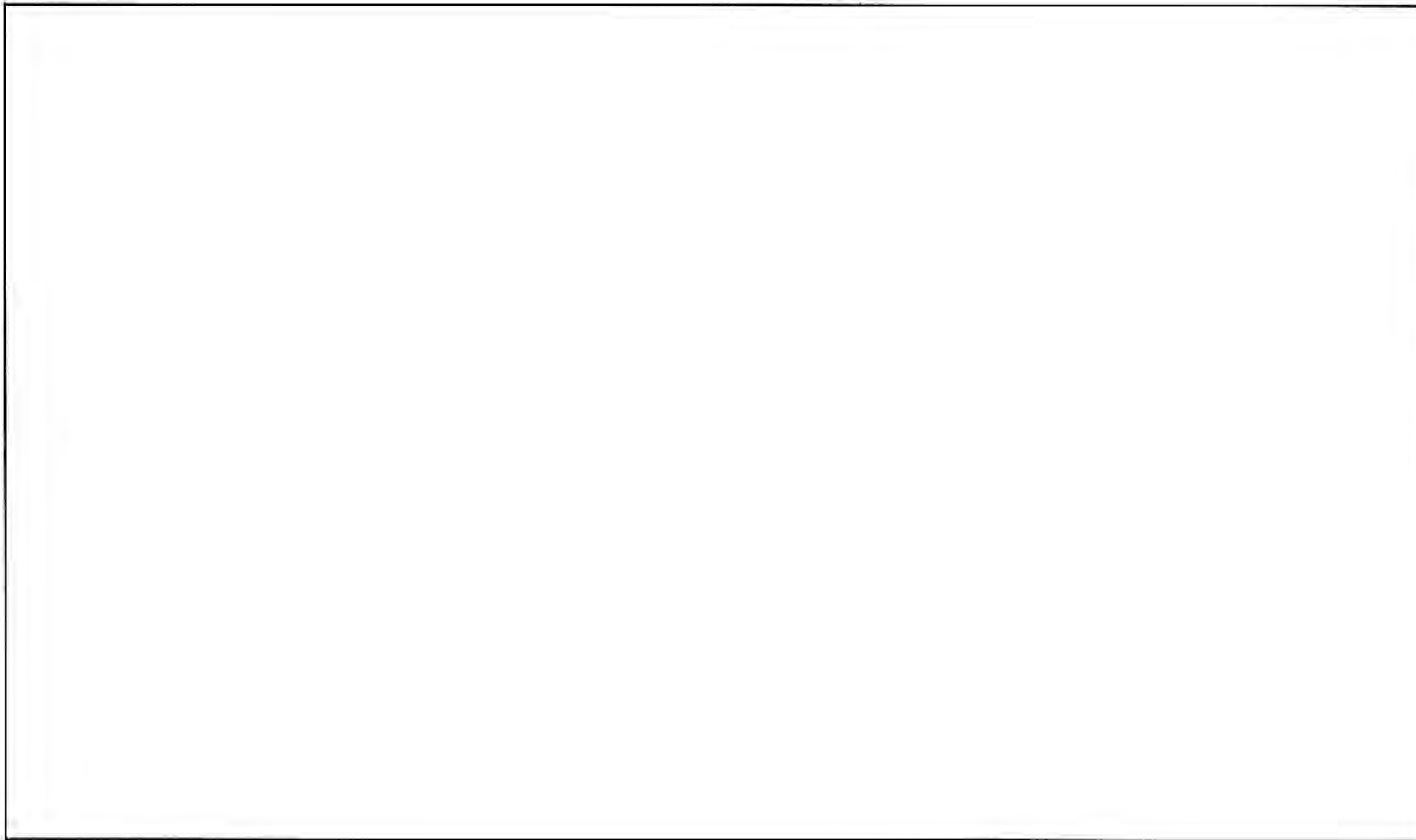


(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET//REL USA, FVEY~~



OCO/DCO-RA Mission Complexity *



* Based on OSD/CAPE and USCYBERCOM staff estimates

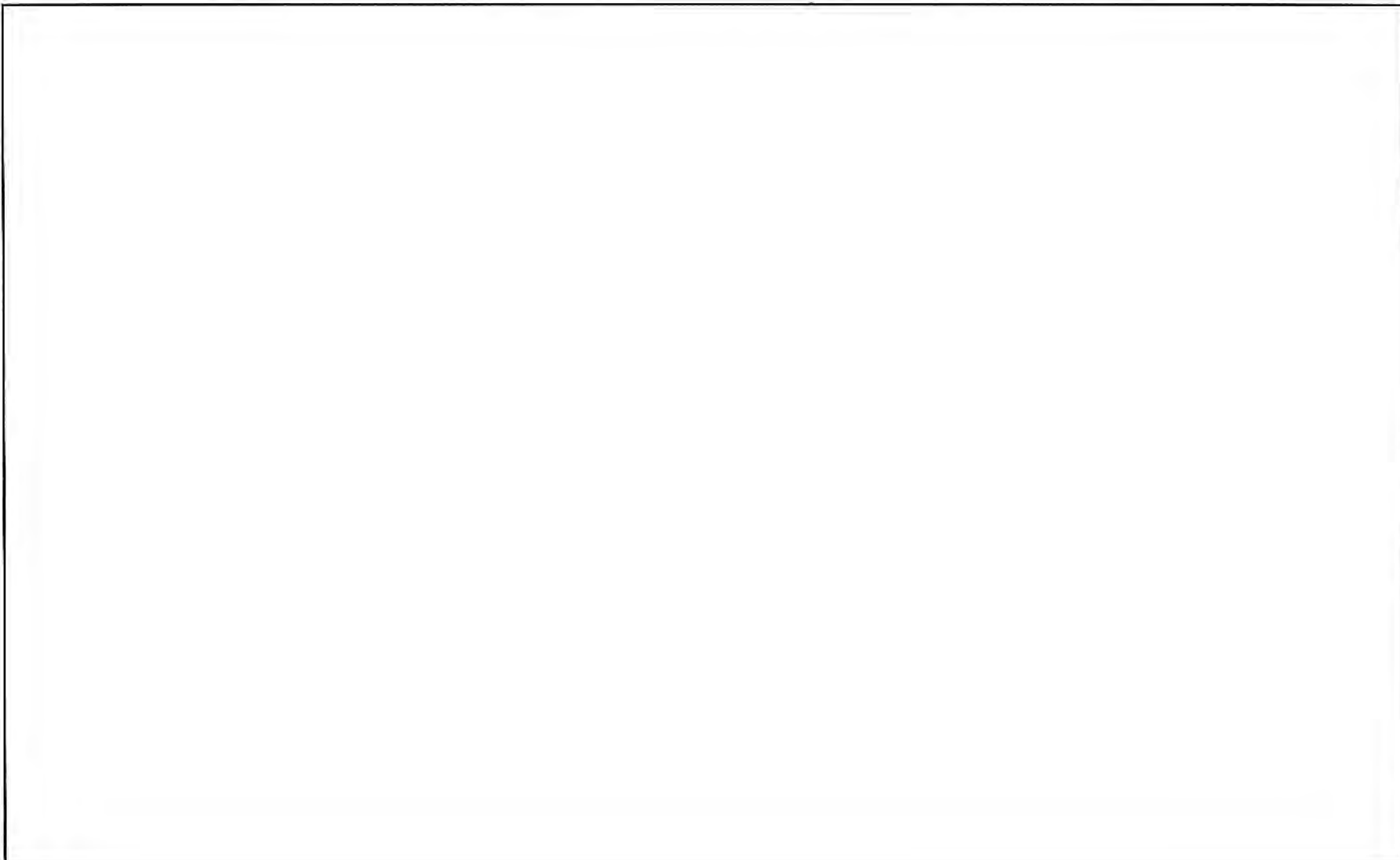
~~SECRET//REL USA, FVEY~~

(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET//REL USA, EYES~~



DCO-IDM & DODIN Ops Assessment

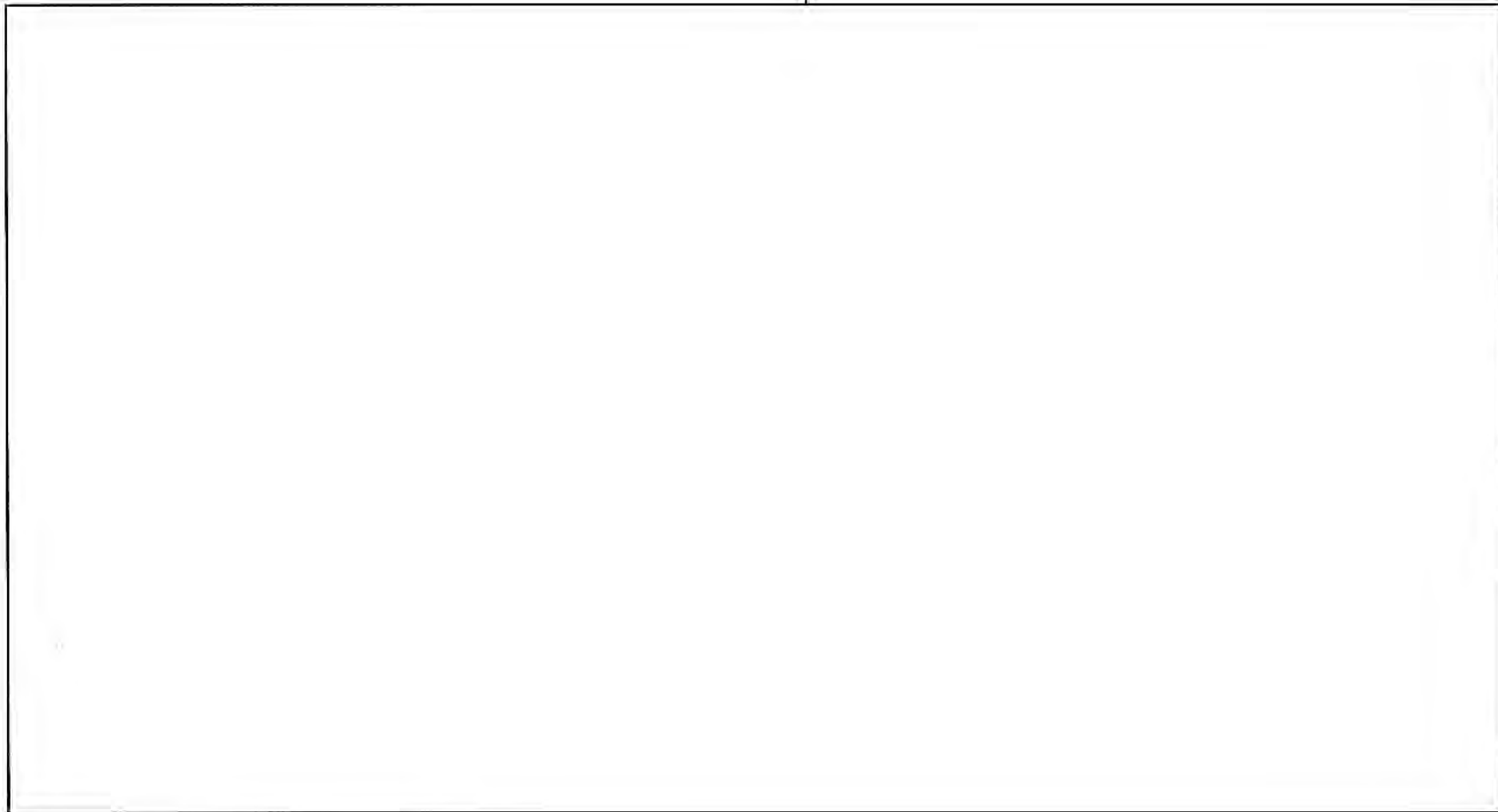


(b) (1) Sec. 1.4 (a)
(b) (5)

~~SECRET//REL USA, CUEV~~



DCO-IDM/DoDIN Ops Complexity *



* Based on OSD/CAPE and USCYBERCOM staff estimates

~~SECRET//REL USA, CUEV~~



Operational Assessment

(b) (1) Sec. 1.4 (a)
(b) (5)





Comments

- ISSUE

- Placeholder
 - Placeholder

- ISSUE

- Place Holder
 - Placeholder

- ISSUE

- Placeholder
 - Place holder

* Based on OSD/CAPE and USCYBERCOM staff estimates

~~SECRET//REL USA, FVEY~~



Backup



* Based on OSD/CAPE and USCYBERCOM staff estimates

~~SECRET//REL USA, FVEY~~

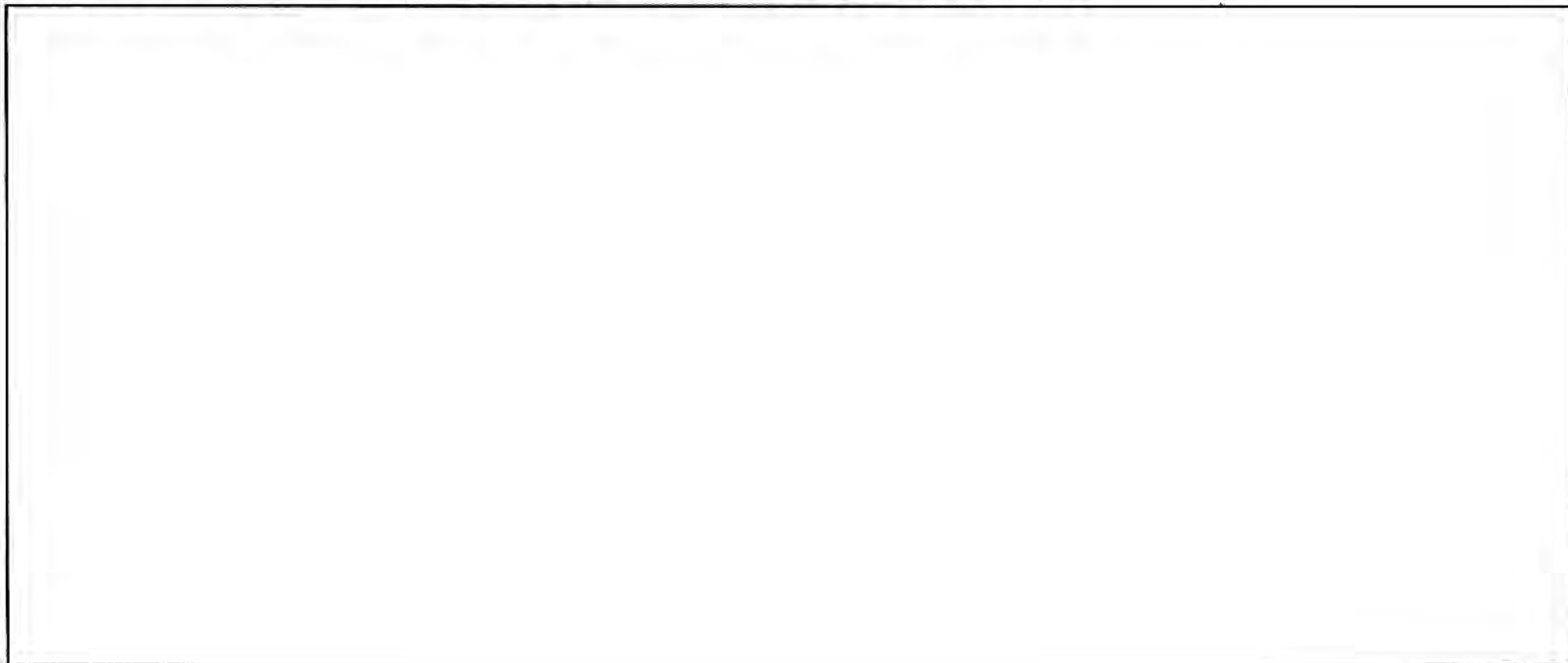


Mission Capacity Assumptions



(b) (1) Sec. 1.4 (a)
(b) (5)

- Internal Cyberspace Operations [DCO-IDM]



* Based on OSD/CAPE and USCYBERCOM staff estimates

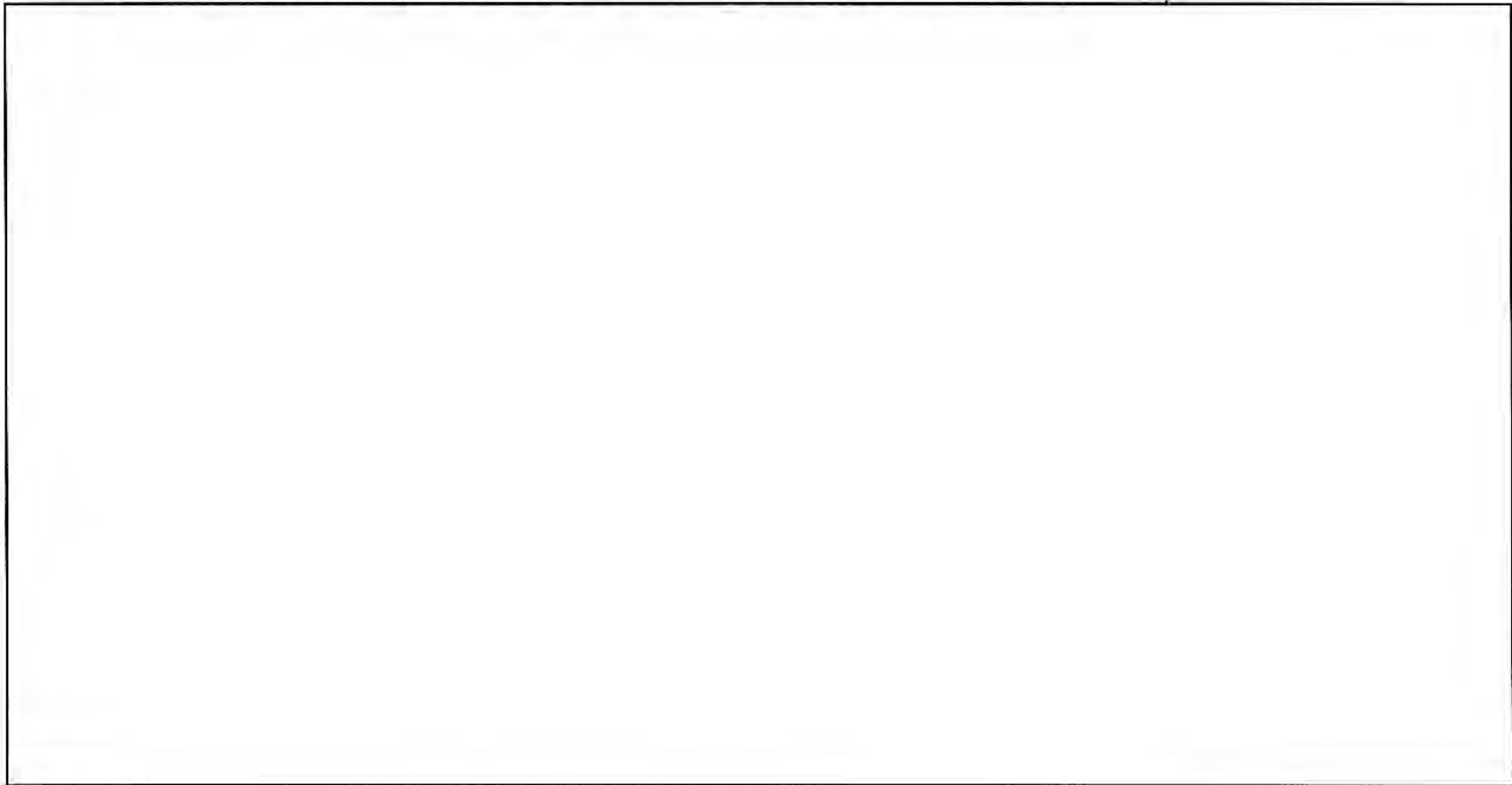


Mission Capacity Assumptions



(b) (1) Sec. 1.4 (a)
(b) (5)

- External Cyberspace Operations [OCO/DCO-RA]



* Based on OSD/CAPE and USCYBERCOM staff estimates



CMF Risk Assessment

(b) (1) Sec. 1.4 (a)
(b) (5)





CPT & NMT FORCE ALLOCATION (FY16)



~~SECRET//REL USA, FVEY~~

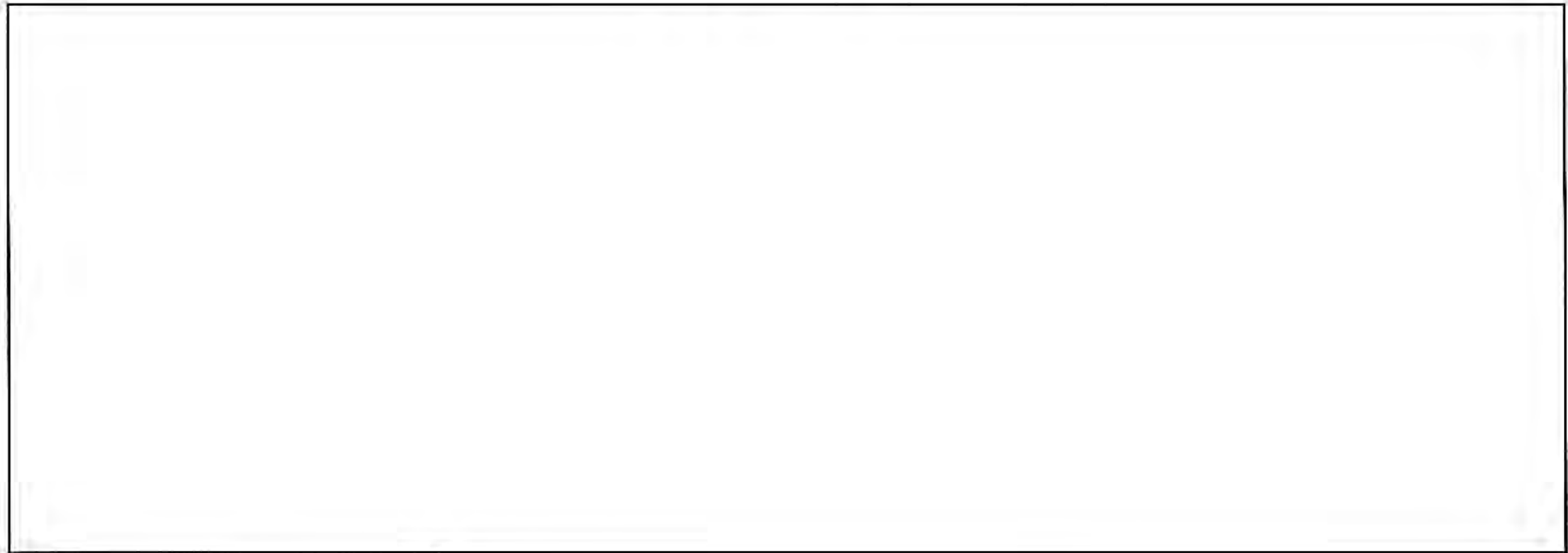
ADJUDICATION INSIGHTS

~~SECRET//REL USA, FVEY~~

Major Topics Agenda

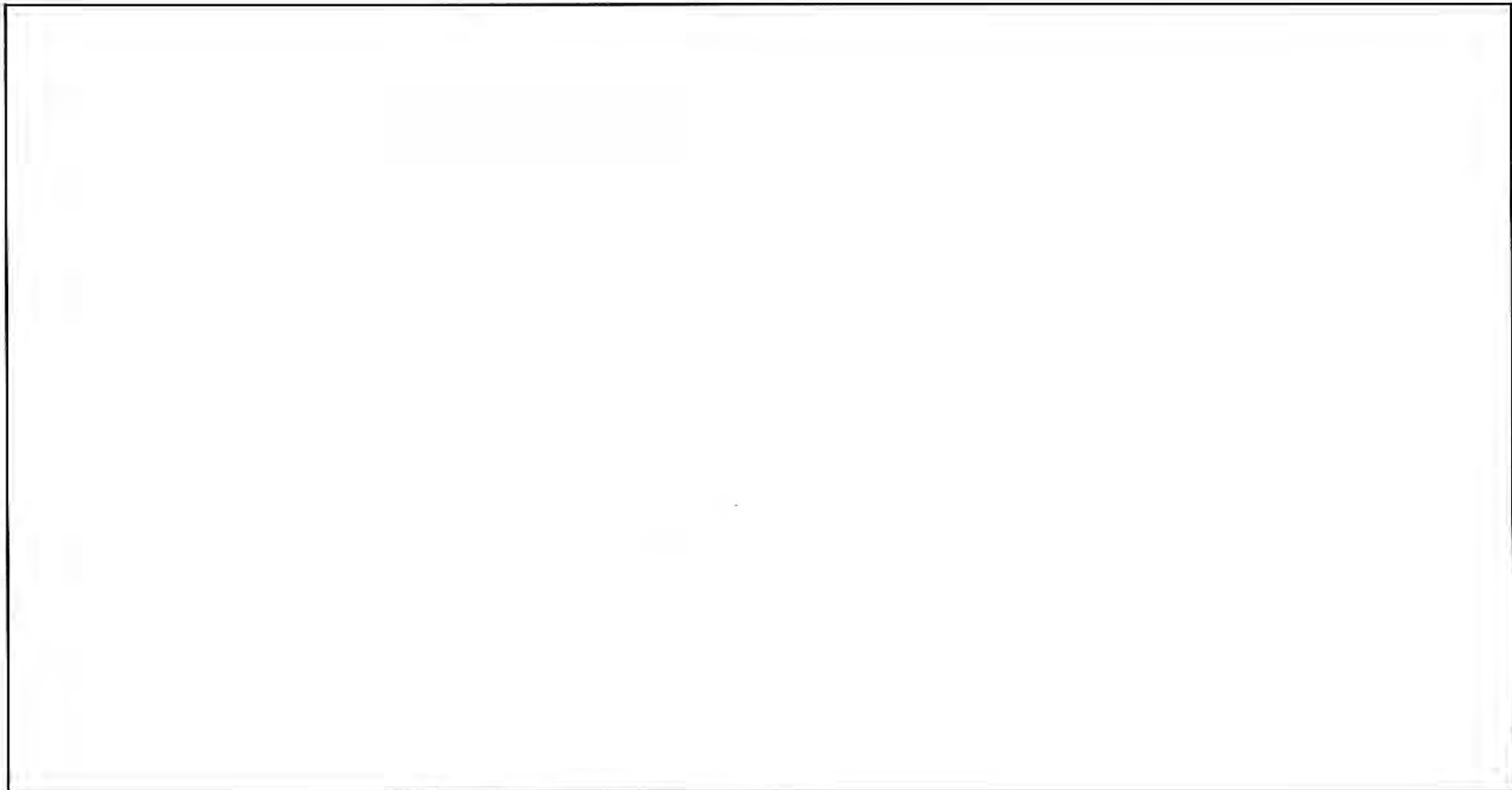
- Visualization of Cyber Forces and Key Terrain
- Global Cyber Force Management
- Cyber Integration with Overall Warfight
- Threat and Operational Risk Assessments
- Interagency C2
- Common metrics
- Deterrence
- Specific terms needing further look

Visualization of Cyber Forces and Key Terrain



(b) (1) Sec. 1.4 (a)
(b) (5)

Global Cyber Force Management



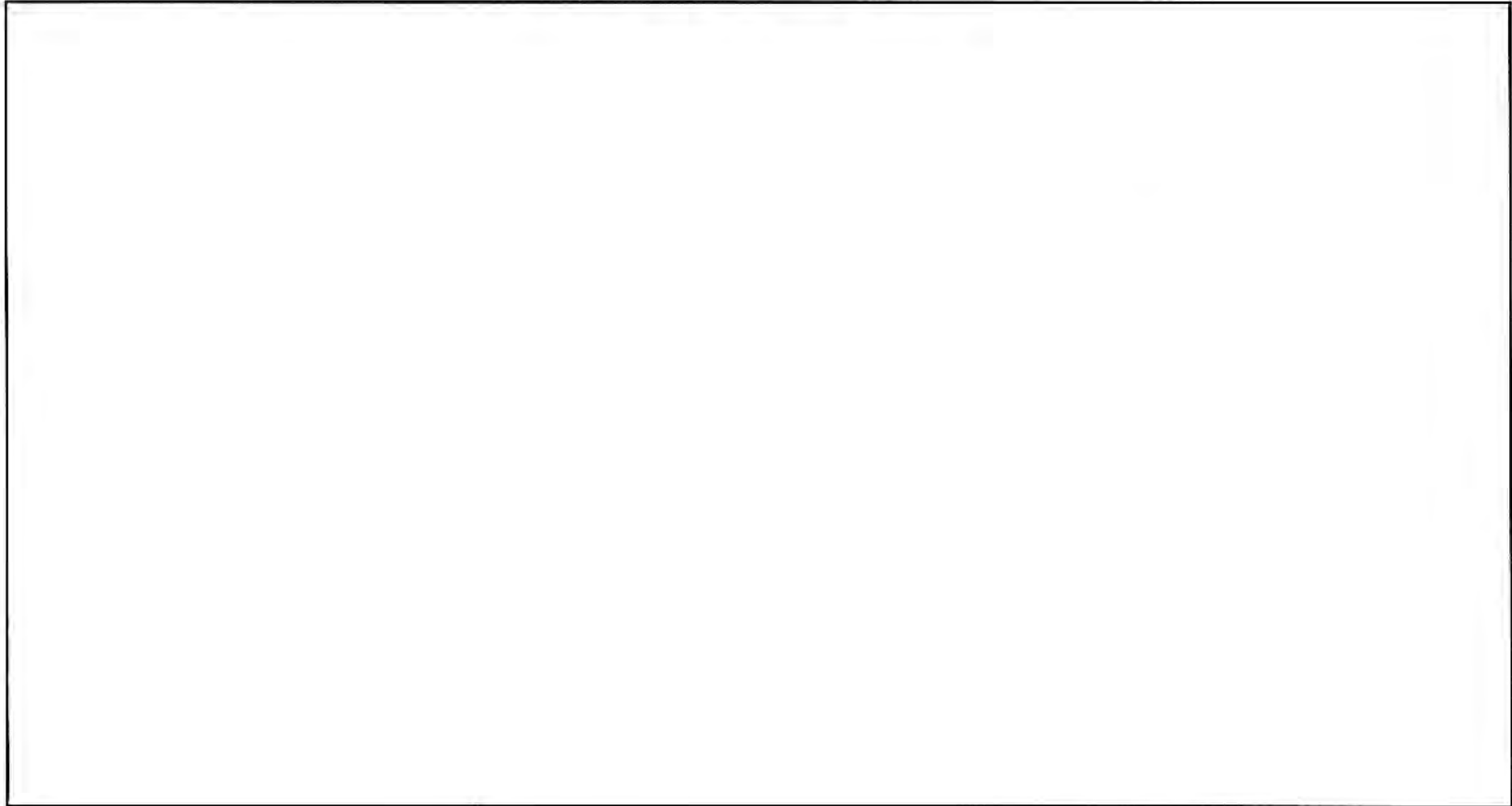
(b) (1) Sec. 1.4 (a)
(b) (5)

Cyber Integration with Warfight

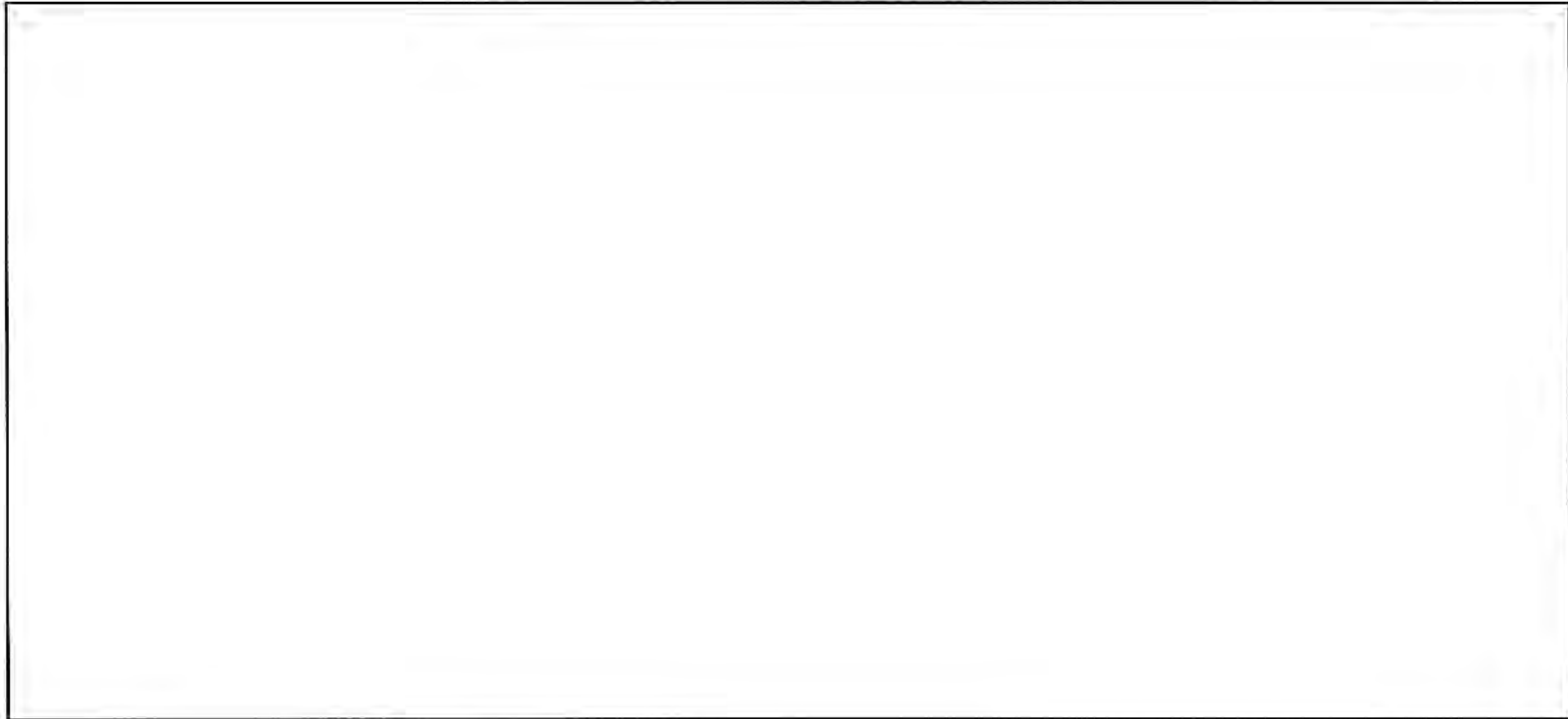


(b) (1) Sec. 1.4 (a)
(b) (5)

Threats and Operational Risk Assessment



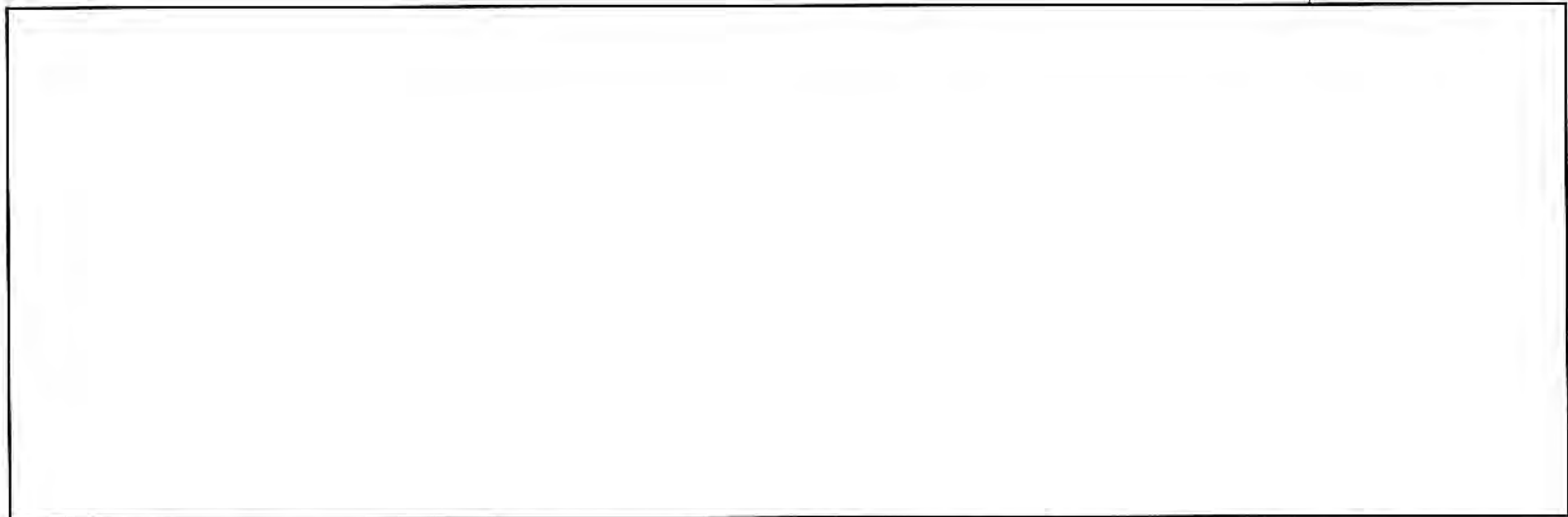
Interagency C2



.....
(b) (1) Sec. 1.4 (a)
(b) (5)

Common Metrics

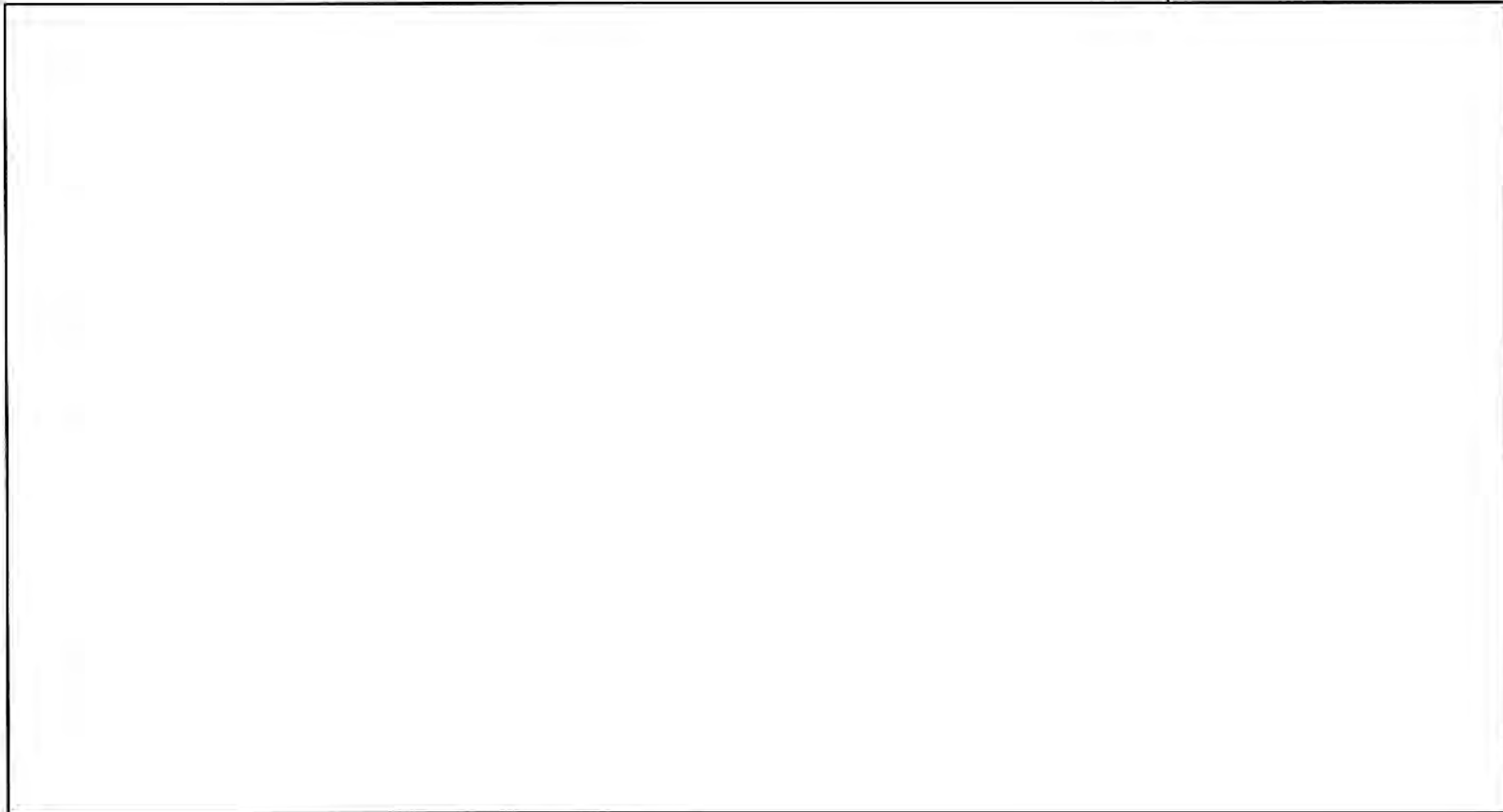
(b) (1) Sec. 1.4 (a)
(b) (5)



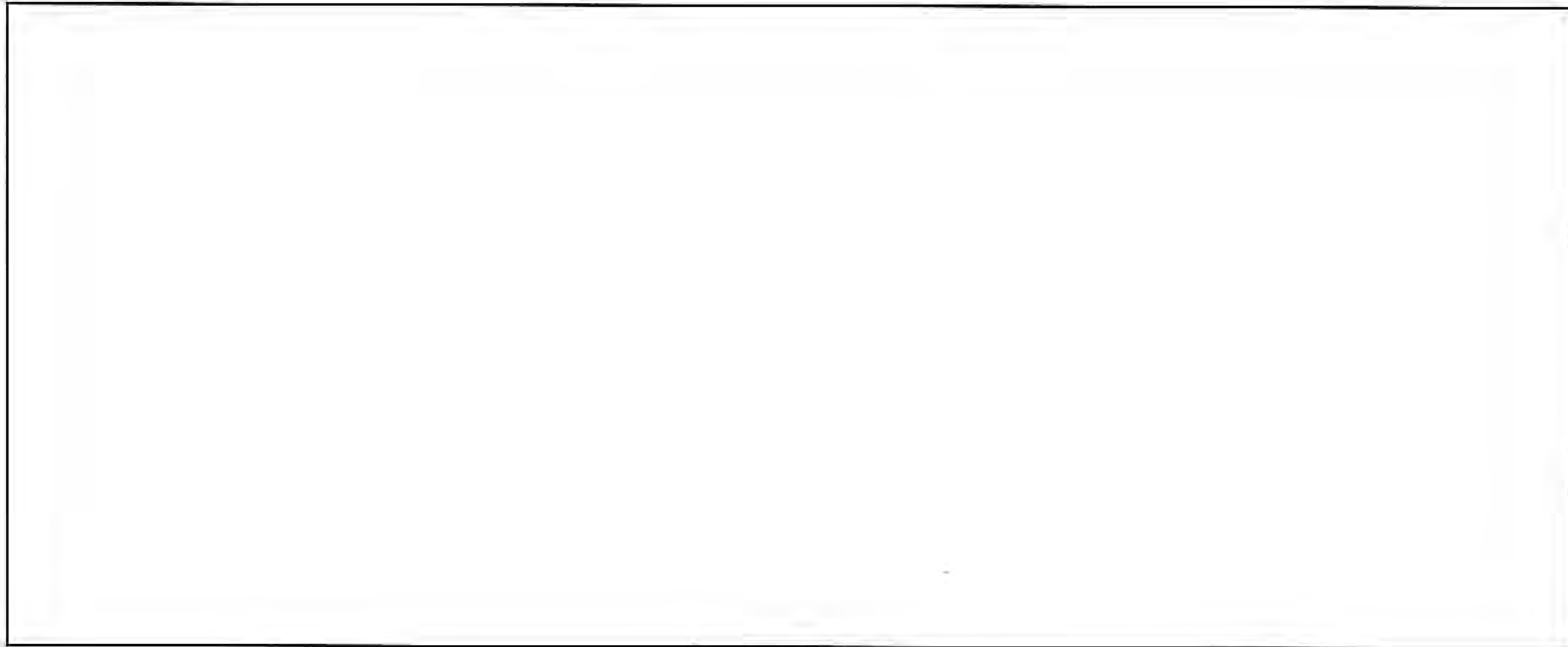
- Game assessment framework developed from SME input...CAPE and CYBERCOM will continue to work

Deterrence

(b) (1) Sec. 1.4 (a)
(b) (5)



Other Thoughts



(b) (1) Sec. 1, 4 (a)
(b) (5)