



UNITED STATES CYBER COMMAND
9800 SAVAGE ROAD, SUITE 6171
FORT GEORGE G. MEADE, MARYLAND 20755

Re: 20-R056

OCT 30 2024

Eric Geller



Dear Mr. Geller,

This letter responds to the enclosed Freedom of Information Act (FOIA) request, submitted to U.S. Cyber Command on July 20, 2020.

We have located and reviewed material responsive to your request. As the Initial Denial Authority, I have determined that the redacted information is exempt from disclosure under the FOIA, title 5, United States Code, section 552(b)(1), (b)(3), (b)(5), and (b)(6). Details of the specific exemptions cited are attached to this letter.

If you are not satisfied with our action on this request, you may seek dispute resolution services from the Department of Defense (DoD) FOIA Public Liaison or the Office of Government Information Services. You also have the right to file an administrative appeal. Contact information for each resource is enclosed.

Dennis Velez

DENNIS VELEZ
Rear Admiral, U.S. Navy
Chief of Staff

Enclosures:
a/s

FOIA Exemptions Cited:*

(b)(1) – information properly and currently classified in the interest of national defense or foreign policy, pursuant to Executive Order 13526, Classified National Security Information;

Section 1.4(a) – military plans, weapons systems, or operations;

Section 1.4(c) – intelligence activities (including covert action), intelligence sources or methods, or cryptology;

Section 1.4(g) – vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security;

Section 1.7(e) – individually unclassified items of information that reveal an additional association or relationship that (1) meets the standards for classification under this order; and (2) is not otherwise revealed in the individual items of information.

(b)(3) – information specifically exempted from disclosure by statute:

10 U.S.C. §130b, personally identifying information of DoD personnel in sensitive units;

18 U.S.C. §798, certain classified information pertaining to the communication intelligence and cryptographic devices of the United States or any foreign government;

50 U.S.C. §3024(i)(1), information pertaining to intelligence sources and methods pursuant to the National Security Act of 1947;

50 U.S.C. §3605, information pertaining to the functions or organization of NSA and certain information pertaining to NSA employees.

(b)(5) – inter- or intra-agency memoranda containing information that qualifies for deliberative process privilege.

(b)(6) – information in personnel and medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

DoD FOIA Public Liaison:

Ms. Toni Fuentes
Phone: (571) 371-0462
Email: osd.foia-liaison@mail.mil

Office of Government Information Services:

Office of Government Information Services
National Archives and Records Administration
8601 Adelphi Road – OGIS
College Park, MD 20740-6001
Email: ogis@nara.gov
Phone: (202) 741-5770
Toll Free: 1-877-684-6448
Fax: (202) 741-5769

Administrative Appeal:**

Ms. Joo Chung
Assistant to the Secretary of Defense for Privacy, Civil Liberties, and Transparency (PCLT)
Office of the Secretary of Defense
4800 Mark Center Drive
ATTN: PCLFD, FOIA Appeals
Mailbox #24
Alexandria, VA 22350-1700
Email: osd.foia-appeal@mail.mil

* The FOIA provides that a federal agency or department may withhold responsive records only if: (1) the agency reasonably foresees that disclosure would harm an interest protected by one of the nine exemptions; or (2) disclosure is prohibited by law. 5 U.S.C. § 552(a)(8)(A)(i). Note that we have considered the foreseeable harm standard when reviewing the records and applying FOIA exemptions. This standard is used to determine whether information may be disclosed even if it technically falls within an exemption.

** Appeal should cite case number above, be clearly marked "FOIA Appeal" and filed within 90 calendar days from the date of this letter.

From: Eric Geller [redacted]
Sent: Monday, July 20, 2020 9:23 AM
To: CYBERCOM_FOIA
Subject: [Non-DoD Source] FOIA request: records about election security war games

Hello,

This is a request under the Freedom of Information Act. I hereby request the following records:

All records of classified and unclassified war games, tabletop exercises, and simulations related to election security (including but not limited to election infrastructure cyberattacks, disinformation, and other forms of election interference) in which U.S. Cyber Command has participated since the 2016 election.

I request a fee waiver as a member of the news media. The requested records are essential to producing journalism that informs the public about government operations. Examples of my work can be found here:
<https://www.politico.com/staff/eric-geller>

If, notwithstanding the waiver, there are any fees for searching, reviewing, or copying the records, please let me know before you task my request. I am willing to pay fees for this request up to a maximum of \$50. If you estimate that the fees will exceed this limit, please inform me first.

If you determine that any of the applicable records is exempt from disclosure, I request a list of those documents as required by *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), cert. denied, 415 U.S. 977 (1972). A "Vaughn index" must describe the withheld documents in enough detail "to permit a reasoned judgment as to whether the material is actually exempt under FOIA." *Founding Church of Scientology v. Bell*, 603 F.2d 945, 949 (D.C. Cir. 1979). In addition, the index must "describe each document or portion thereof withheld, and for each withholding it must discuss the consequences of supplying the sought-after information." *King v. U.S. Dep't of Justice*, 830 F.2d 210, 223-24 (D.C. Cir. 1987). Furthermore, "the withholding agency must supply 'a relatively detailed justification, specifically identifying the reasons why a particular exemption is relevant and correlating those claims with the particular part of a withheld document to which they apply.'" *Id.* at 224 (citing *Mead Data Central v. U.S. Dep't of the Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977)).

If some of the records I request are exempt from disclosure, please provide to me all reasonably segregable non-exempt sections of these records. See 5 U.S.C. § 552(b). If a document contains such non-exempt sections, but you assert that they are spread out across the document in such a way that segregation would be impossible, please explain which sections of the document are non-exempt and how those sections are spread out across the document. *Mead Data Central*, 566 F.2d at 261. If you make a claim that a section is non-segregable, you must provide the same level of detail as described above for a Vaughn index. If you deny my request entirely, please state that it is not appropriate to segregate sections of the records for disclosure.

I would prefer to receive all correspondence and records electronically, but if that is not possible, my physical address is:

Eric Geller
[redacted]

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 20 business days, as the statute requires.

—
Eric Geller
Cybersecurity Reporter
POLITICO



Document 1

SECRET//NOFORN

(b) (1) Sec. 1.4(a)
(b) (3) 50 U.S.C. §3605

TTX
Narrative
ESG Update to GEN Nakasone
29 Apr 2020

BLUF	ESG, with USCYBERCOM [] is developing TTX scenarios accounting for [] [] First event will be on 30 Apr, USCYBERCOM "Staff Academics" with TTXs to follow.
WHY	[] [] In order to ensure processes run smooth when the time comes for 2020 U.S. election mission packages, the command will sponsor and conduct a series of TTX.
HOW	The ESG, ICW USCYBERCOM [] is designing a TTX schedule with vignettes for the following interest items: [] The team will scope TTXs at certain levels (AOs, O-6/GS-15, GO/FO, and interagency principals). The TTX schedule will align to the ESG campaign timeline.
WAY AHEAD	USCYBERCOM Staff Academics Session scheduled for 30 Apr Agenda includes: ESG Update, [] [] Attendees: • ESG [] • USCYBERCOM Staff: [] • Component [] • CO-IPs [] • Task Forces: [] TTX schedule will follow (number of TTXs, scenarios, participants, agenda).

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

SECRET//NOFORN

Document 2

~~SECRET~~
FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY

AO TTX

Election Security Scenario

As of: 25 June 2020

FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY
~~SECRET~~

SECRET

I. (U) General

- (U) Participants
 - USCYBERCOMMAND
 - Cyber National Mission Force
 - National Security Agency
 - NSA/CSS Cybersecurity Operations Center (NCSOC)
 - National Security Operations Center (NSOC)
 - [REDACTED]
 - Department of Homeland Security Cybersecurity and Infrastructure Security Agency
 - Department of State Operations Center
 - Federal Bureau of Investigation CyWatch
 - Department of Treasury
 - Department of Justice
 - Office of the Director of National Intelligence
 - [REDACTED]
- (U) USCYBERCOM Points of Contact
 - US CYBERCOM [REDACTED]
 - [REDACTED]
 - USCYBERCOM [REDACTED]
 - US CYBERCOM [REDACTED]
 - [REDACTED]
- (U) CNMF Points of Contact
 - Election Security Group [REDACTED]
 - Election Security Group [REDACTED]
 - CNMF [REDACTED]

3. (U) Exercise Purpose

(U//FOUO) Exercise policies and procedures that enable the DOD alongside Interagency Partners to respond to a major cyberspace attack against Critical Infrastructure/Key Resources (CIKR) impacting the 2020 Presidential Elections.

4. (U) Training Objective

(S//REL) Understand and practice the processes of information sharing in the context of election security.

- [REDACTED]
- [REDACTED]
- [REDACTED]

(U) PROLOG

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

FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY
SECRET

SECRET

FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY

(S) Foreign adversaries conducted cyberspace operations to influence the United States 2018 midterm elections. Our adversaries still want to interfere with our democratic process and are expected to continue conducting cyberspace operations to effect the 2020 Presidential Election.

(S) USCYBERCOM and the Interagency formed Election Security Groups to combat this interference and conducted a number of Cyber Effects Operations leading up to the 2020 Presidential Election to mitigate the threats.

(U//FOUO) **STARTEX Conditions**

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

(U) **Exercise Injects**

(S) [REDACTED]

<Discuss Blue Player Actions>

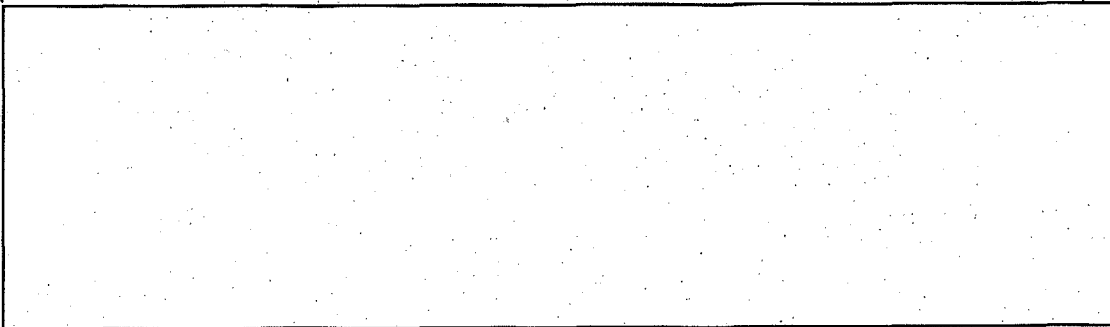
(U//FOUO) [REDACTED]

<Discuss Blue Player Actions>

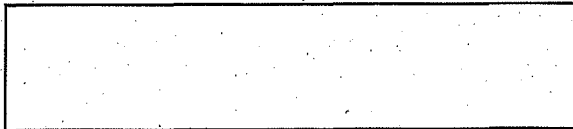
(b) (5)

~~SECRET~~

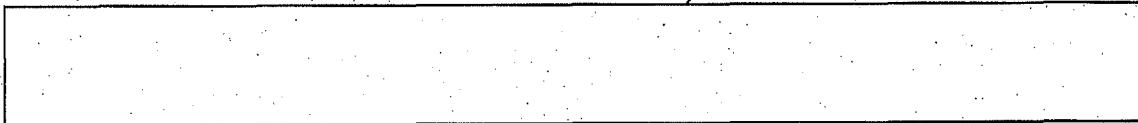
FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY



<Discuss Blue Player Actions>

- 
-
-



<Discuss Blue Player Actions/Equities>



<Discuss Blue Player Actions>

- While this is going on, the Staff does what?

(U//~~FOUO~~) **ENDEX/HOTWASH**

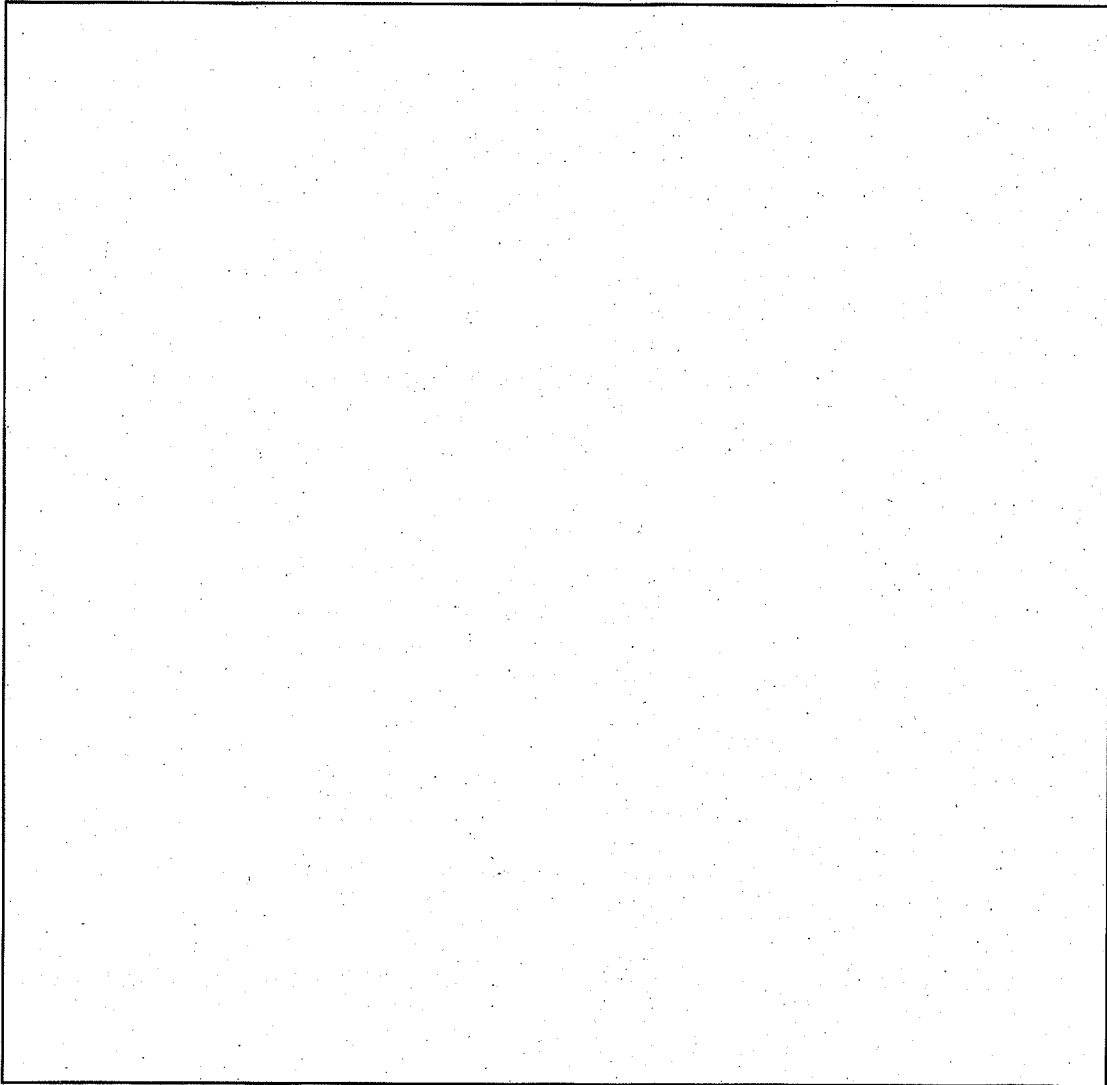
- USCYBERCOMMAND
 - Cyber National Mission Force
- National Security Agency
 - NSA/CSS Cybersecurity Operations Center (NCSOC)
 - National Security Operations Center (NSOC)
- 
- Department of Homeland Security Cybersecurity and Infrastructure Security Agency
- Department of State Operations Center
- Federal Bureau of Investigation CyWatch
- Department of Treasury
- Department of Justice
- Office of the Director of National Intelligence
- 

SECRET

FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY

NOTES:

For TTX scenario build-out, the leads are Reach out to them soonest to distill a plan for getting a scenario built.. Goal should be one scenario that progresses with multiple injects that tease out the topics we originally suggested. Over to the AO collective as to battle rhythm necessary to achieve maximum training.



(b) (3) 50 U.S.C. §3605

(b) (5)

TOP SECRET//SI//REL TO USA, FVEY

FOR TRAINING USE ONLY / FOR TRAINING USE ONLY / FOR TRAINING USE ONLY
SECRET

Document 3

Academic Session


28 APR 20 Update

(b) (3) 50 U.S.C. §3605

(b) (6)

The overall classification of this briefing is:

TOP SECRET//SI//ORCON//NOFORN

Classified by: 
Derived from: NSA/CSSM 1-52
Dated: 20191204





TTX Academic Session Agenda

1. 29 APR N4 brief- Focus on slides 6 and 7

2. ESG Participants / agenda

3.

4.

5.



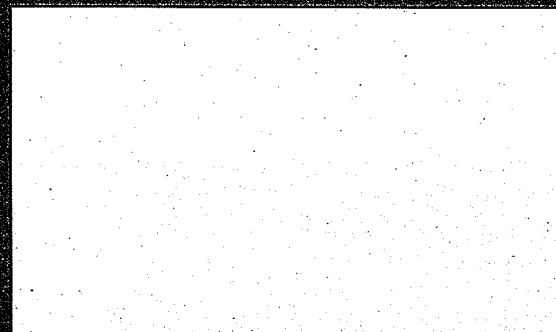


EXECUTIVE SUMMARY

AGENDA

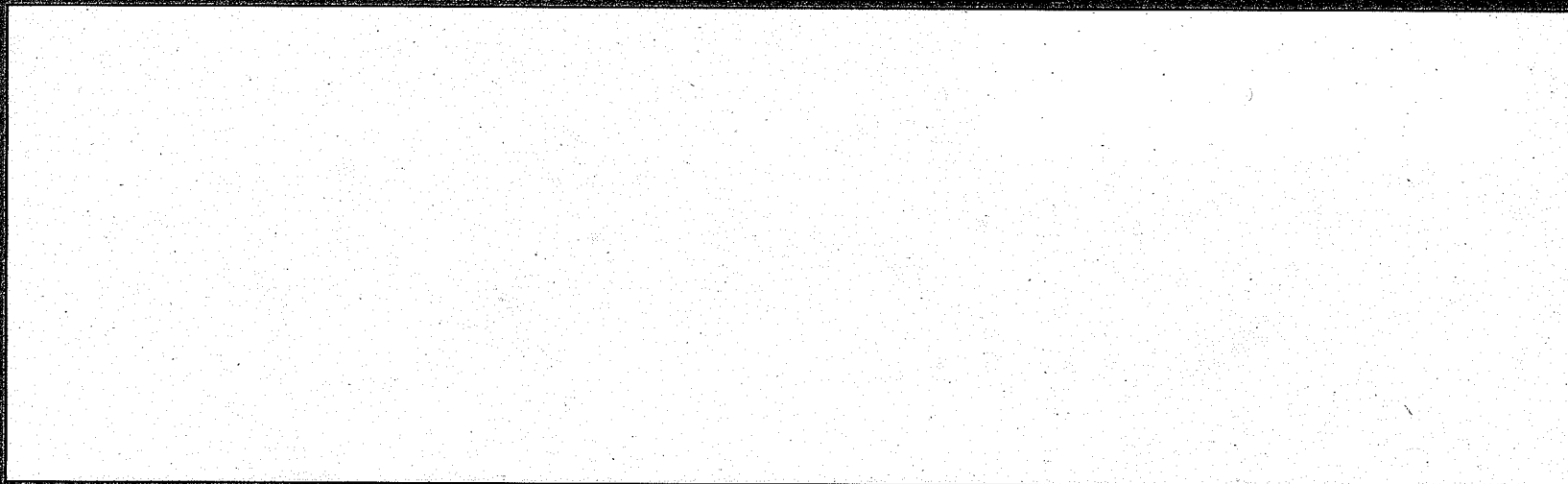
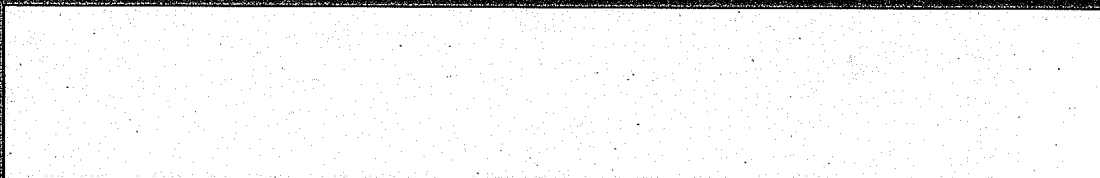
- Counter-Interference
- Setting the Force
- Operational Timeline
- Designing a CEO TTX

SIGNIFICANT UPDATES



ELECTION
SECURITY GROUP

INVESTING IN COUNTER-INTERFERENCE





SETTING THE FORCE

Increase speed to action; enable partners

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

(b) (3) 50 U.S.C. §3605



OPERATIONAL SYNCHRONIZATION

(b) (1) Sec. 1.4(a) (c) (g), (b) (3) 18 U.S.C. §798, (b) (3) 50 U.S.C. §3024(i), (b) (3) 50 U.S.C. §3605





EFFECTS OPERATIONS TTX

Exercise Mission Package Coordination & Approval Through Execution

- Key Functions:



- Key Players:

- Near term: USCYBERCOM Staff, CO-IPEs CNMF, JFHQ-Cs, TFs, CO-IPEs



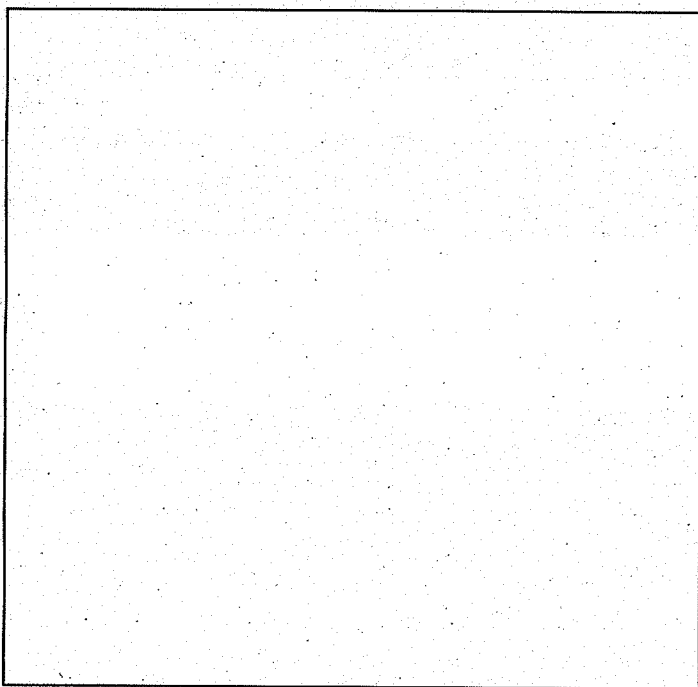
- Events:

- 30 APR Staff Academics
- MAY AO level TTX
- JUN O-6/GS-15 TTX
- MID JUL GO/FO/Agency Principals TTX

TOP SECRET//SI//NOFORN

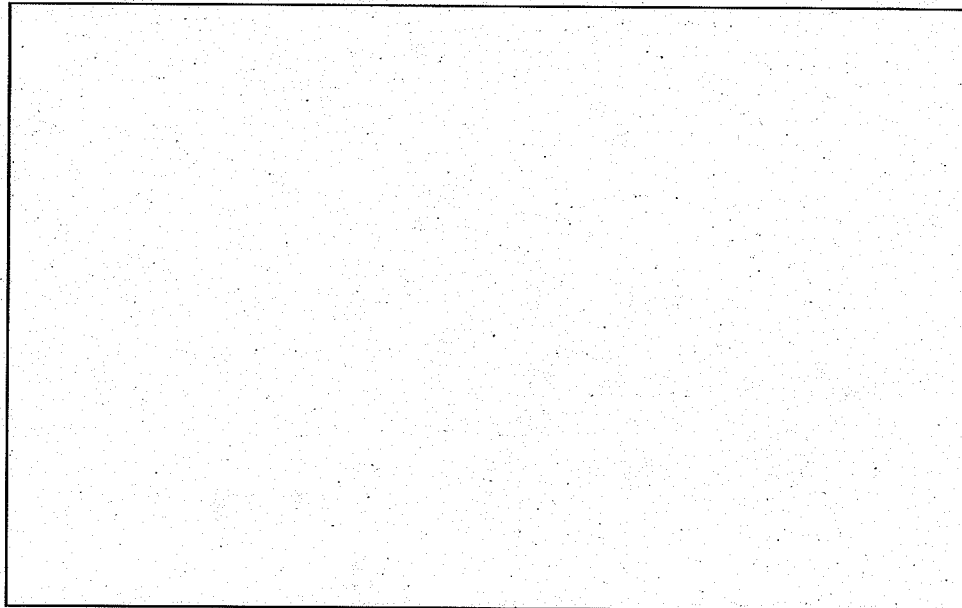


ESG Staff Sync/Academics - Thursday 4/30



(b) (3) 10 U.S.C. §130b
(b) (6)

Refined Agenda



(b) (3) 10 U.S.C. §130b
(b) (5)
(b) (6)

SECRET//REL TO USA, FVEY

ELECTION
2020

CAO: 26APR20

SECRET//REL TO USA, FVEY

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

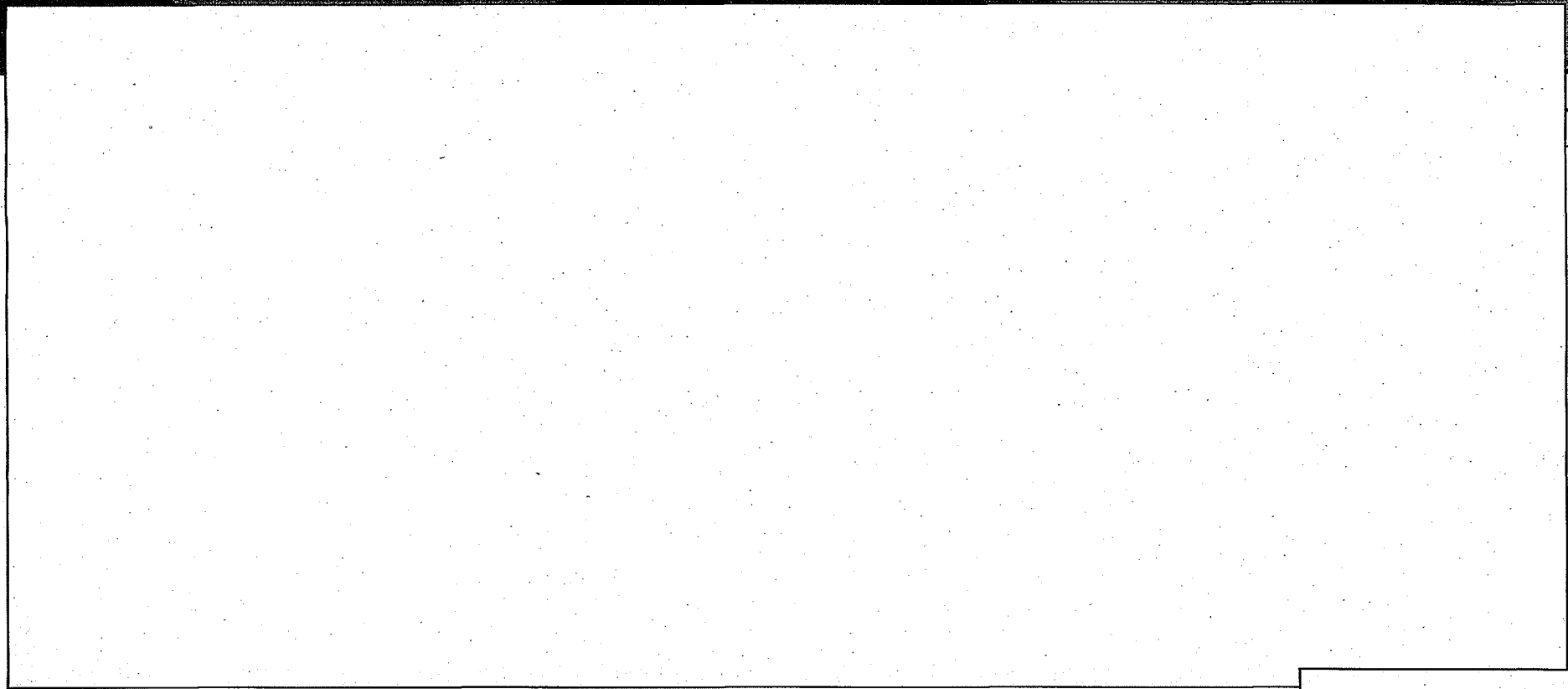
SECRET//REL TO USA, FVEY

ELECTION
2020

SECRET//REL TO USA, FVEY

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

SECRET//NOFORN//NOVA



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

SECRET//NOFORN//NOVA

SECRET//REL TO USA, FVEY

----- (b) (1) Sec: 1.4(a)

SECRET//REL TO USA, FVEY

SECRET//REL TO USA, FVEY

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

SECRET//REL TO USA, FVEY

Legend

→ Direct Coordination
← Indirect Coordination

SECRET//REL TO USA, FVEY

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

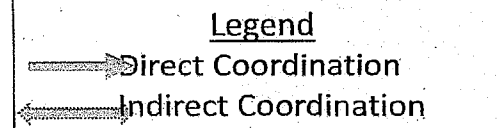
SECRET//REL TO USA, FVEY

Legend

→ Direct Coordination
← Indirect Coordination

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

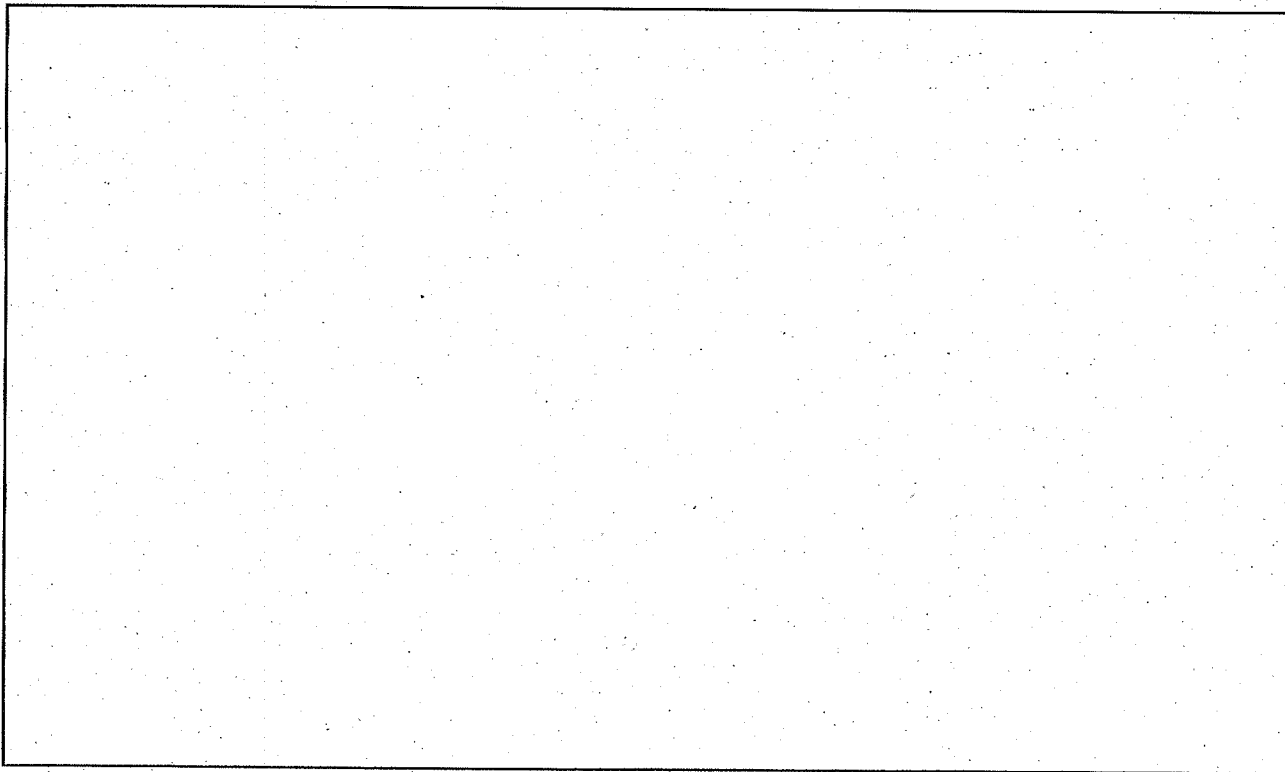
SECRET//REL TO USA, FVEY





SECRET//NOFORN

(U) USCYBERCOM CEO Planning and Approval



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

SECRET//NOFORN

Document 4

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



(b) (3) 50 U.S.C. 53605

NSA/CNMF TTX
Tue 7 Aug 0800



Prep for DHS Elections TTX
13-15 Aug

This Exercise is Classified

~~SECRET//REL TO USA, CVEV~~

Classified By
Derived From: NSA/CSSM 1-52
Dated: 20130930
Declassify On: 20401234

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Agenda

(U) 0800 Welcome & Introductions

(U) Leadership Comments

(U)

(b) (3) 50 U.S.C. §3605

(U) DHS TTX Objectives & NSA/CNMF TTX Objectives

(U) **0830 STARTEX**

(U) 0945-1000 Break

(U) 1150 Closing Remarks

(U) Are the NSA/CNMF reps attending the DHS TTX fully prepped?

(U) Are the folks in the room ready to propose & implement solutions by 1 SEPT 2018?

(U) Can NSA/CNMF deliver on the options presented to higher leadership?

(U) **1200 ENDEX**

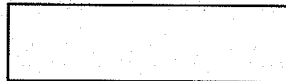
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Venue Information



(U//~~FOUO~~) NSA



(b) (3) 50 U.S.C. §3605

(U//~~FOUO~~) Phones

(U) Restrooms

(U) Directions to vending machines and cafeterias

(U//~~FOUO~~) Security: Classified discussion is authorized up to

TOP SECRET//SI//NOFORN level

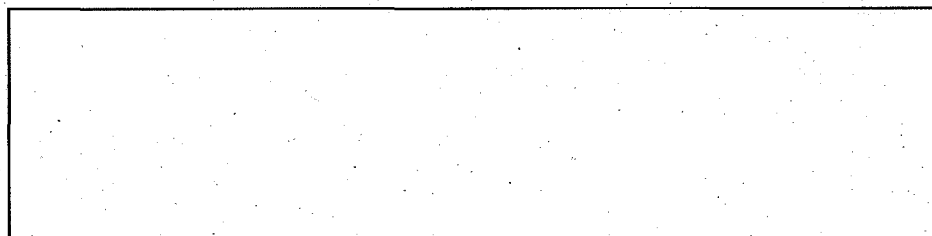
(U//~~FOUO~~) Unless you have courier authorization and materials, please turn in all classified notes at ENDEX if you are departing NSA-W

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



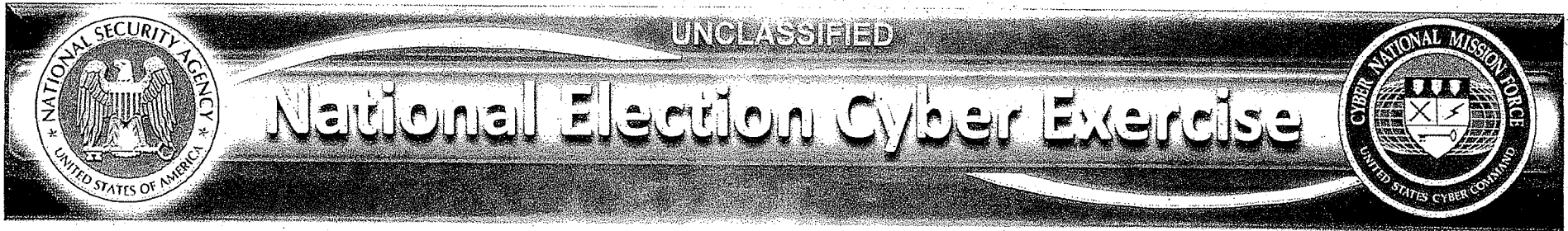
Brig Gen Timothy Haugh, USAF

CNMF Commander



----- (b) (3) 50 U.S.C. §3605

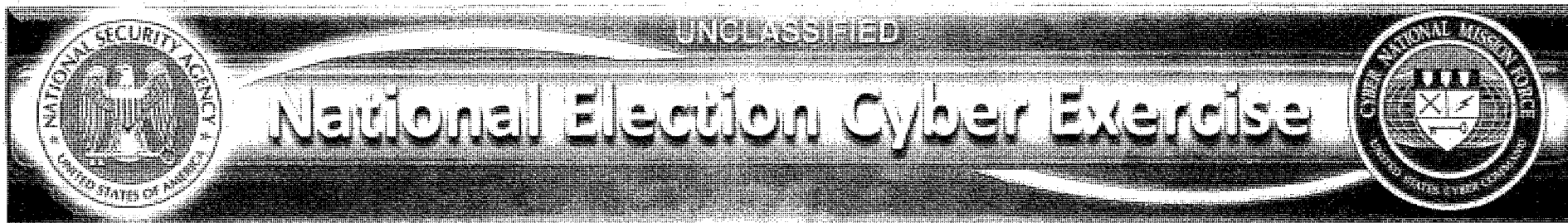
UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



DHS TTX Purpose

(U) Identify best practices and areas for improvement in cyber incident planning, preparedness, identification, response, and recovery through simulation of a realistic scenario exploring impacts to voter confidence, voting operations, and the integrity of elections.

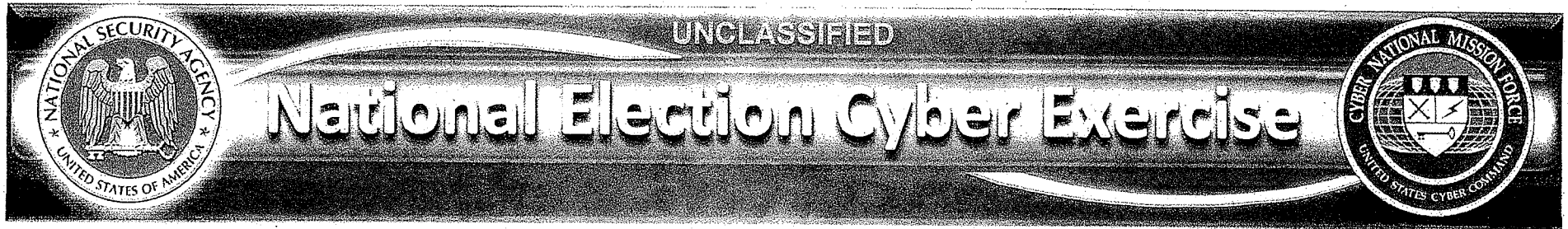
UNCLASSIFIED



DHS TTX Objectives

1. (U) Discuss the preparedness of state and county boards of election to respond to and manage cybersecurity incidents.
2. (U) Discuss processes for identifying potential cybersecurity incidents or issues.
3. (U) Examine information sharing processes amongst state and county boards of election and with state and federal partners.
4. (U) Explore processes for requesting state/federal incident response resources once county/state resources are exhausted.

UNCLASSIFIED



DHS TTX Objectives

5. Increase understanding of Federal cyber risk management resources and incident response roles, responsibilities, and coordination processes.
6. Explore processes for addressing news and social media manipulation related to the conduct of elections.
7. Inform the development of state and country-level processes and plans to address elections-related cyber incidents.

UNCLASSIFIED



UNCLASSIFIED//FOR OFFICIAL USE ONLY

NSA/CNMF TTX Objectives



(U//~~FOUO~~) **Purpose:** Identify capabilities and gaps/shortfalls

(U//~~FOUO~~) **Ensure inputs and outputs to inter/intra-agency processes are known**

(U//~~FOUO~~) Identify decision points, decision makers, decision deadlines and which organization has what for action

(U//~~FOUO~~) Formulate responses at strategic/operational levels

(U//~~FOUO~~) Prep attendees for the DHS TTX

(U//~~FOUO~~)

(U//~~FOUO~~) **Participants:** NSA, USCYBERCOM/CNMF SMEs, and appropriate LNO's

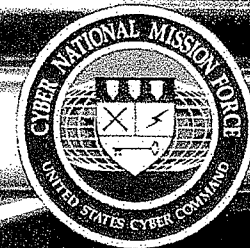
(b) (3) 50 U.S.C. §3605

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED//FOR OFFICIAL USE ONLY

NSA/CNMF Support Provided



1. (U//FOUO)

2. (U//FOUO)

3. (U//FOUO)

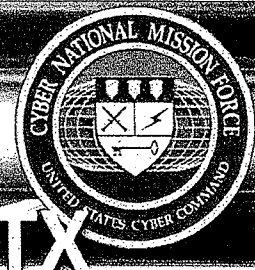
4. (U//FOUO)

5. (U//FOUO)

6. (U//FOUO)



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Factors to Consider To frame your thinking during the TTX

(U//~~FOUO~~) What are NSA/CNMF responses for or reacting to

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~) What questions does NSA/CNMF want to push to DHS?

(U//~~FOUO~~) What questions does NSA/CNMF want DHS to ask States?

(U//~~FOUO~~) What do our partners (State/Guard/DHS) expect of us?

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~) Are all authorities/agreements in place?



UNCLASSIFIED

National Election Cyber Exercise



DHS "Tabletop The Vote 2018" Brochure

MODULE 1: INFORMATION SHARING

MODULE 2: INCIDENT IDENTIFICATION

MODULE 3: INCIDENT RESPONSE

16 DHS TTX injects over 10 slides

30+ Pre-staged Questions

3 Hours to complete

Let's Begin

UNCLASSIFIED



UNCLASSIFIED//FOR OFFICIAL USE ONLY

Module 1 Information Sharing

4 Sept 2018 - Inject



(U) A technical alert is released by the DHS National Cybersecurity and Communications Integration Center (NCCIC)/FBI and forwarded by the Multi-State Information Sharing and Analysis Center (MS-ISAC)/Election Infrastructure Information Sharing and Analysis Center (EI-ISAC) regarding [REDACTED]

[REDACTED]

(b) (5)

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED//FOR OFFICIAL USE ONLY



Module 1 Information Sharing

4 Sept 2018 - Questions

(U//~~FOUO~~)

(U//~~FOUO~~) How do we know we supplied valuable information?
Are we prepared to receive feedback?

(U//~~FOUO~~)

(U//~~FOUO~~) Are we receiving information from DHS? Is DHS
notifying the right POCs? What is Ops Center threshold to care?

(U//~~FOUO~~) Do we have attribution to a foreign entity?

(b) (3) 50 U.S.C. §3605

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLAS

Module 1 – Information Sharing

7/14 Sept 2018 - Inject



(U)

[Redacted content]

(U)

[Redacted content]

(b) (5)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



UNCLASSIFIED//FOR OFFICIAL USE ONLY



Module 1 – Information Sharing

7/14 Sept 2018 - Questions

(U//FOUO)

(b) (5)

(U//FOUO) How does DHS prioritize this activity of

(U//FOUO)

(U//FOUO) Will DHS and FBI engage with private industry?

(b) (3) 50 U.S.C. §3605

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Module 1 – Information Sharing

18/26 Sept 2018 - Inject



(U)

[Redacted]

[Redacted]

(U)

[Redacted]

[Redacted]

(b) (5)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



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



Module 1 – Information Sharing

18/26 Sept 2018 - Questions

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(~~S~~//REL TO USA, FVEY)

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

(b) (3) 50 U.S.C. §3605

(b) (5)

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



Module 2 – Incident Identification

6 Oct 2018




(U)




(b) (5)

UNCLASSIFIED

UNCLASSIFIED



Module 2 – Incident Identification



6 Oct 2018 - Questions

(U//FOUO) [REDACTED]

[REDACTED]

(U//FOUO) Should we expect DHS to request DOD conduct offensive operations?

(b) (3) 50 U.S.C. §3605

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



UNCLASSIFIED

Module 2 – Incident Identification

8/16 Oct 2018 - Injects



(U)

--

(U)

--

(b) (5)

UNCLASSIFIED



UNCLASSIFIED

Module 2 - Incident Identification

18 Oct 2018 - Injects



(U)

[Redacted]

[Redacted]

(U)

[Redacted]

[Redacted]

(b) (5)

UNCLASSIFIED



UNCLASSIFIED

Module 2 – Incident Identification



18 Oct 2018 - Questions

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

(U//~~FOUO~~)

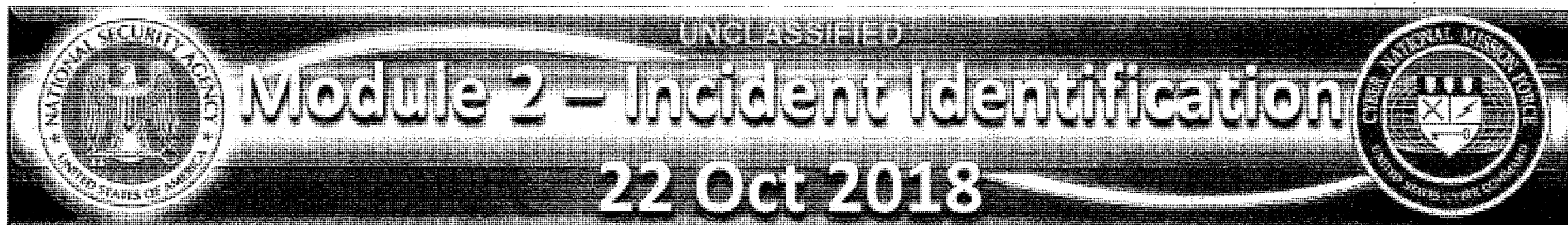
(U//~~FOUO~~)

(U//~~FOUO~~)

(b) (3) 50 U.S.C. §3605

(b) (5)

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



(U)

(b) (5)

UNCLASSIFIED



UNCLASSIFIED

Module 3 – Incident Response

5/6 Nov 2018 - Injects



(U)

[Redacted]

[Redacted]

(U)

[Redacted]

[Redacted]

(b) (5)

UNCLASSIFIED



UNCLASSIFIED

FOR OFFICIAL USE ONLY



Module 2 – Incident Identification

18 Oct 2018 - Questions

(U//~~FOUO~~)

[Redacted]

(U//~~FOUO~~)

[Redacted]

[Redacted]

(U//~~FOUO~~)

[Redacted]

(b) (3) 50 U.S.C. §3605

(b) (5)

UNCLASSIFIED//FOR OFFICIAL USE ONLY



UNCLASSIFIED

Module 3 – Incident Response

6 Nov 2018 - Injects



(U)

[Redacted content]

(U)

[Redacted content]

(b) (5)

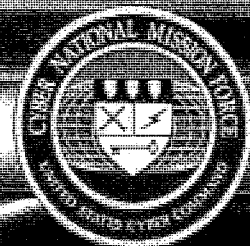
UNCLASSIFIED



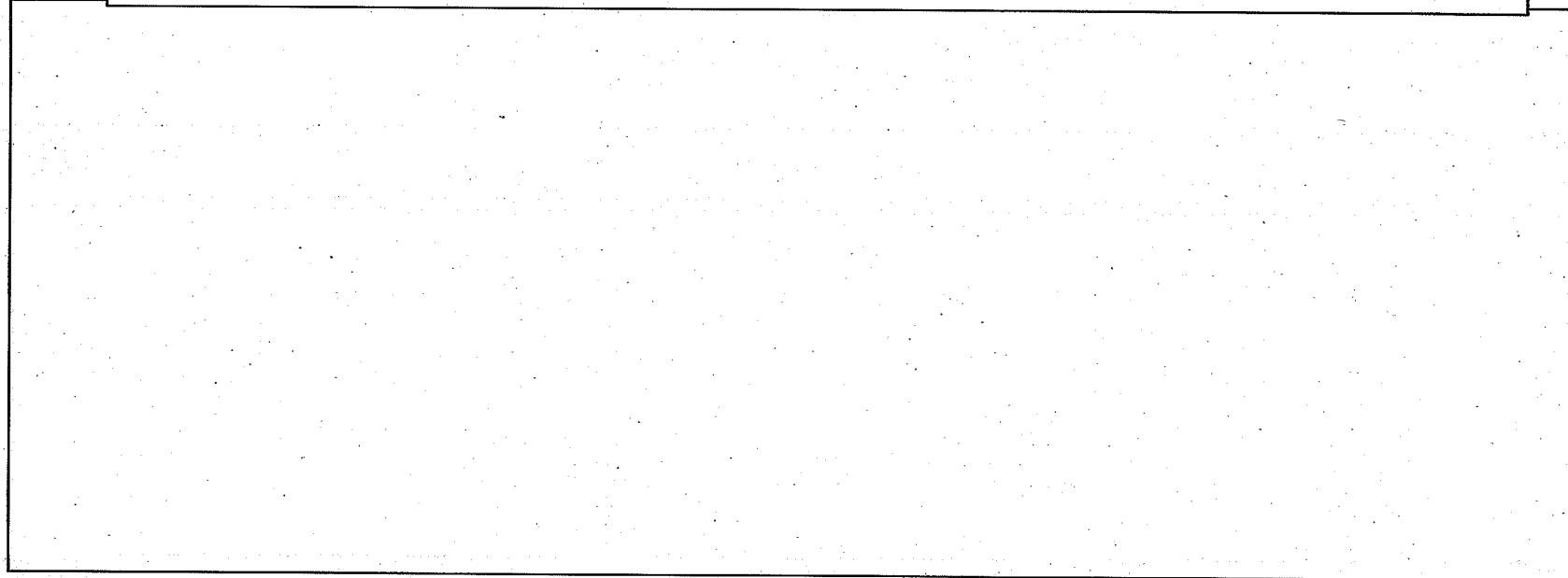
UNCLASSIFIED

Module 3 – Incident Response

6 Nov 2018 - Injects



(U)



(b) (5)

UNCLASSIFIED



UNCLASSIFIED//FOR OFFICIAL USE ONLY



So, Can We Deliver These?

1. (U//FOUO)

[Redacted]

2. (U//FOUO)

[Redacted]

3. (U//FOUO)

[Redacted]

4. (U//FOUO)

[Redacted]

5. (U//FOUO)

[Redacted]

6. (U//FOUO)

[Redacted]

(b) (3) 50 U.S.C. §3605

(b) (5)

UNCLASSIFIED//FOR OFFICIAL USE ONLY



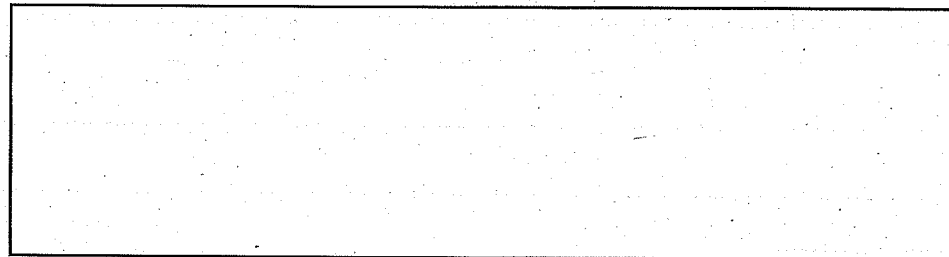
UNCLASSIFIED

Wrapup / Final Remarks



Brig Gen Timothy Haugh, USAF

CNMF Commander



(b) (3) 50 U.S.C. §3605

UNCLASSIFIED

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



Thank You!

This Exercise is Classified

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

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~



UNCLASSIFIED

Backup Slides



BACKUP SLIDES

UNCLASSIFIED



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

TTX Objective



(b) (3) 50 U.S.C. §3605

(U//~~FOUO~~) Evaluate community's ability to

[Redacted]

(U//~~FOUO~~) ID capabilities and gaps/shortfalls

(U//~~FOUO~~) View via perspective of

[Redacted]

[Redacted]

[Redacted]

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

(b) (3) 50 U.S.C. §3024(i), (b) (3) 50 U.S.C. §3605

(b) (5)

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

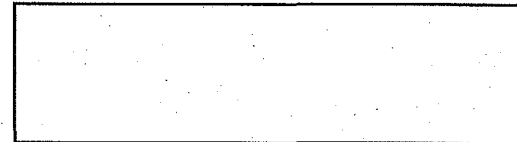
Document 5



(b) (3) 10 U.S.C. §130b

(b) (6)

2020 OCO Elections TTX



The overall classification of this briefing is: _____

Classified By [REDACTED]
Derived From: USCYBERCOM SCG
Dated: 20160615
Declassify On: ~~20420229~~

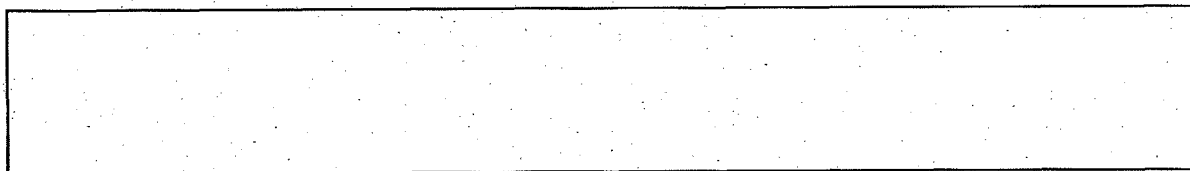


Agenda

- Welcome (b) (3) 10 U.S.C. §130b
(b) (6)
- White Cell Intro
- Introductions
- CDR Intent (PME)
- TTX Rules of Engagement
- Objectives
- Facts & Assumptions
- Timeline
- Academics
- Scenario Overview
- Scenario 1 Execution
 - Inputs & Outputs
- References
- Formal Outbrief: TBD (14 or 15 Nov)



Welcome



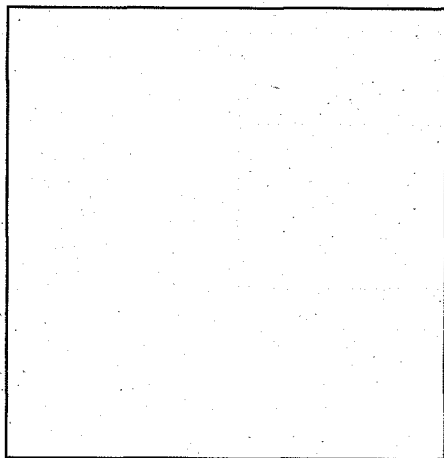
(b) (3) 10 U.S.C. §130b

(b) (6)

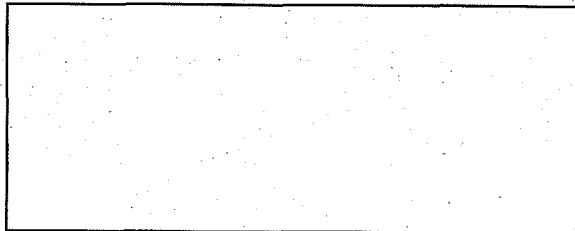


White Cell Intro

- JFHQ-C (AF) (NSA-W)



- JFHQ-C (AF) (NSA-T)



(b) (3) 10 U.S.C. §130b

(b) (6)



Around the Room Introductions

- Name, Org, Duty Location
- JFHQ-C (AF)
- CNMF
- USCC
- USEUCOM
- VTC
- Others



CDR Intent/PME

(b) (1) 1.4 (a)

- CDR Intent: Understand JFHQ-C (AF) and CNMF planning, execution and coordinating processes and procedures ISO the 2020 Elections across JFHQ-C (AF), CNMF, USCC, and USEUCOM.
- Purpose: Identify CCMD, JFHQ-C (AF), and CNMF CEO assessment gaps ISO of the 2020 Elections.
- Method: Conduct an AO TTX to simulate execution operations ISO of 2020 Elections. O-6 Level will be held in December (tentatively).
- End State: JFHQ-C (AF), CNMF, USCC, USEUCOM developed common understanding of CEO processes and procedures ISO U.S. 2020 Elections.



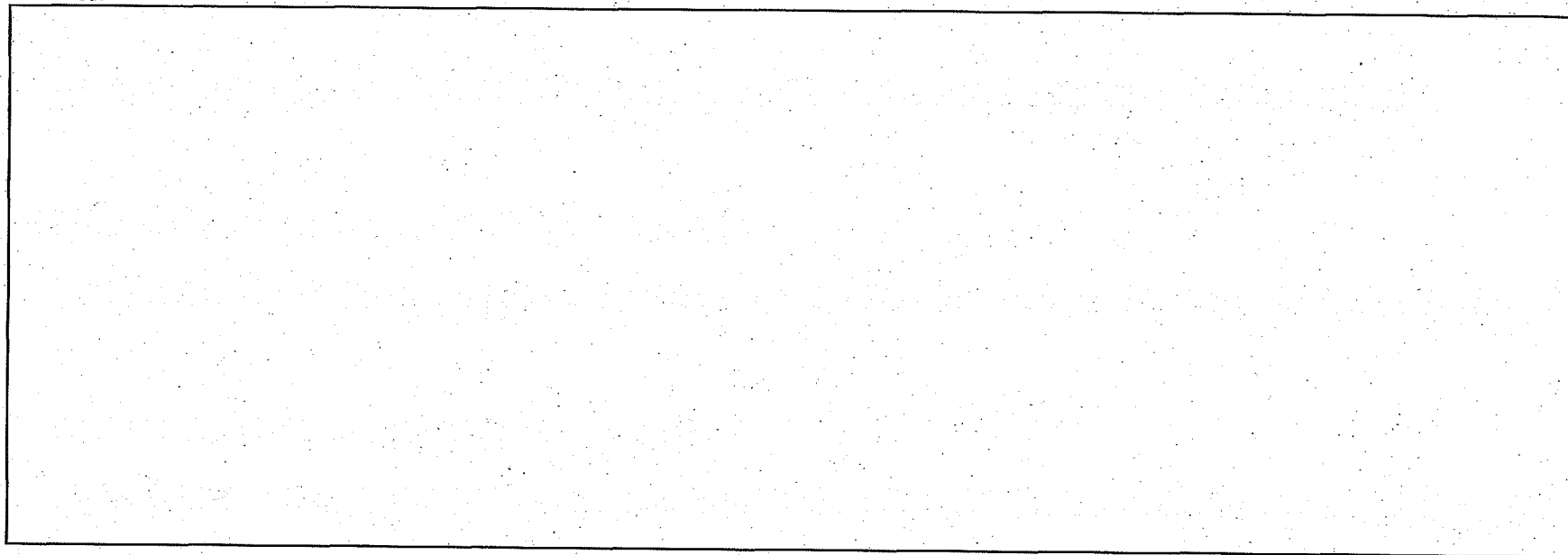
TTX Rules of Engagement

- Due to limited time, White Cell members will hold the team to an aggressive schedule
- The "Parking Lot" is for topics requiring further discussion
- "Parking Lot" topics will be addressed at the end of the TTX (time permitting) or in other forums
- Participants will follow White Cell guidance and will be mindful of timelines (avoid rabbit holes!)
- Focus on Operational Level Processes vs tactical execution



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

Objectives



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

(b) (5)

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



Participants

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

- **USCC**

- [Redacted]

- **JFHQ-C (AF)**

- [Redacted]

- **CNMF**

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- **USEUCOM**

- **CO-IPE, JCC**



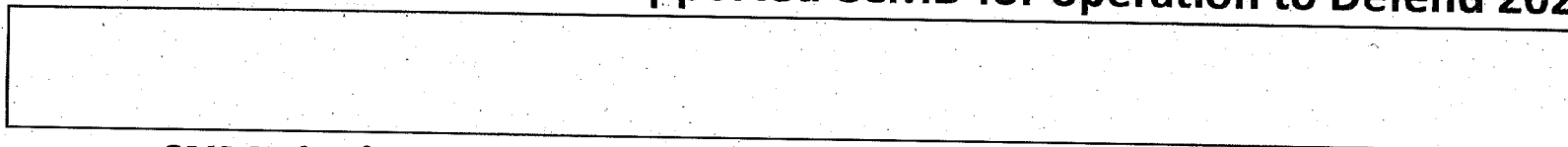
~~SECRET//REL TO USA, FVEY~~

Facts & Assumptions

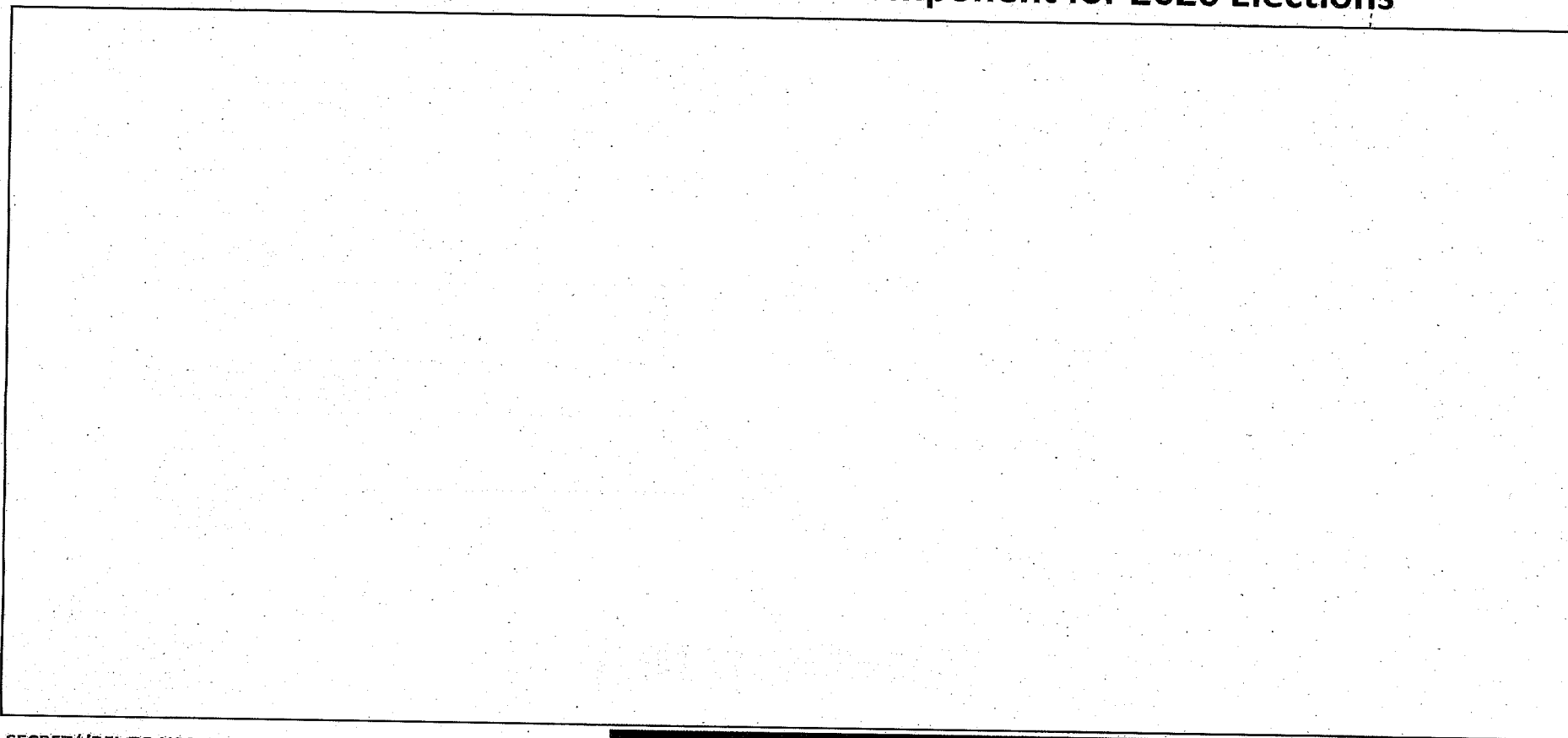
(b) (1) Sec. 1.4(a)

- **Facts**

- **USCYBERCOM is the supported CCMD for operation to Defend 2020 Elections**



- **CNMF is the supported USCYBERCOM component for 2020 Elections**



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



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

Timeline & Agenda

12 November:

- Small Break Out Sessions (as required/requested/more info to come)
 - [redacted] 1300-1400 (Large Conf Room)
 - [redacted] 1400-1500 (Lg Conf Room)
 - [redacted] (SKYPE)

(b) (1) Sec. 1.4(a)
(b) (3) 10 U.S.C. §130b
(b) (6)

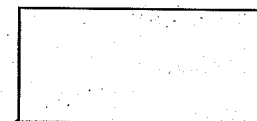
13 November: (ICC)

- 0730: Welcome
- 0800: Scenario 1 Begin
- 0930-0950: Break (White Cell Meeting)
- 0950-1030: Scenario 1 Cont.
- 1030-1040: Break
- 1040: Scenario 1 Cont.
- 1100: Lunch
- 1300: Scenario 1 Cont.
- 1430-1445: Break
- 1600: TTX Due Outs/Closing Comments
- Formal Outbrief: TBD (14 or 15 Nov)

Rooms:
NSA-W
ICC:



NSA-T



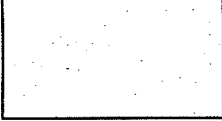

(b) (3) 50 U.S.C. §3605

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



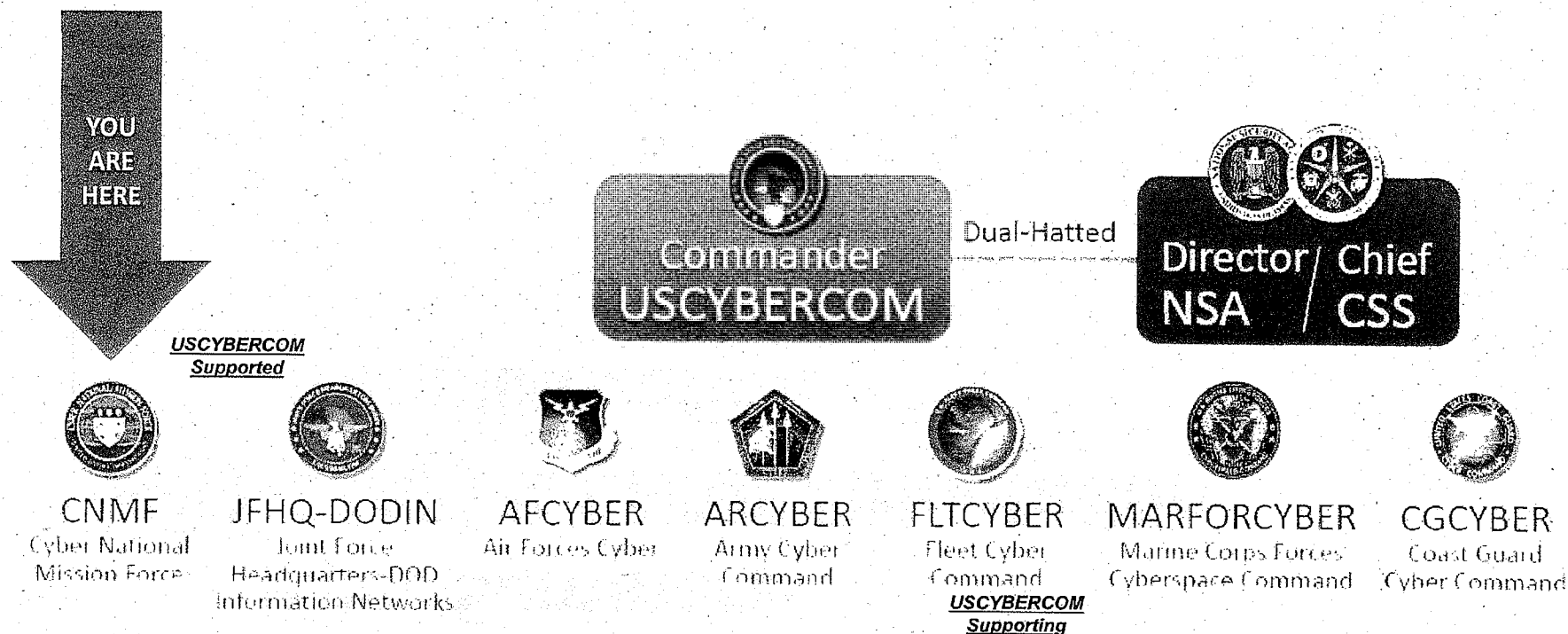
Academics

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

-  Exec Summary
- JFHQ-C (AF) & CNMF Orientation
-  Familiarization



CNMF - Where We Fit



**WE HACK THE HACKERS
WE DO EVERYTHING WITH PARTNERS
OUR MISSION IS GLOBAL**

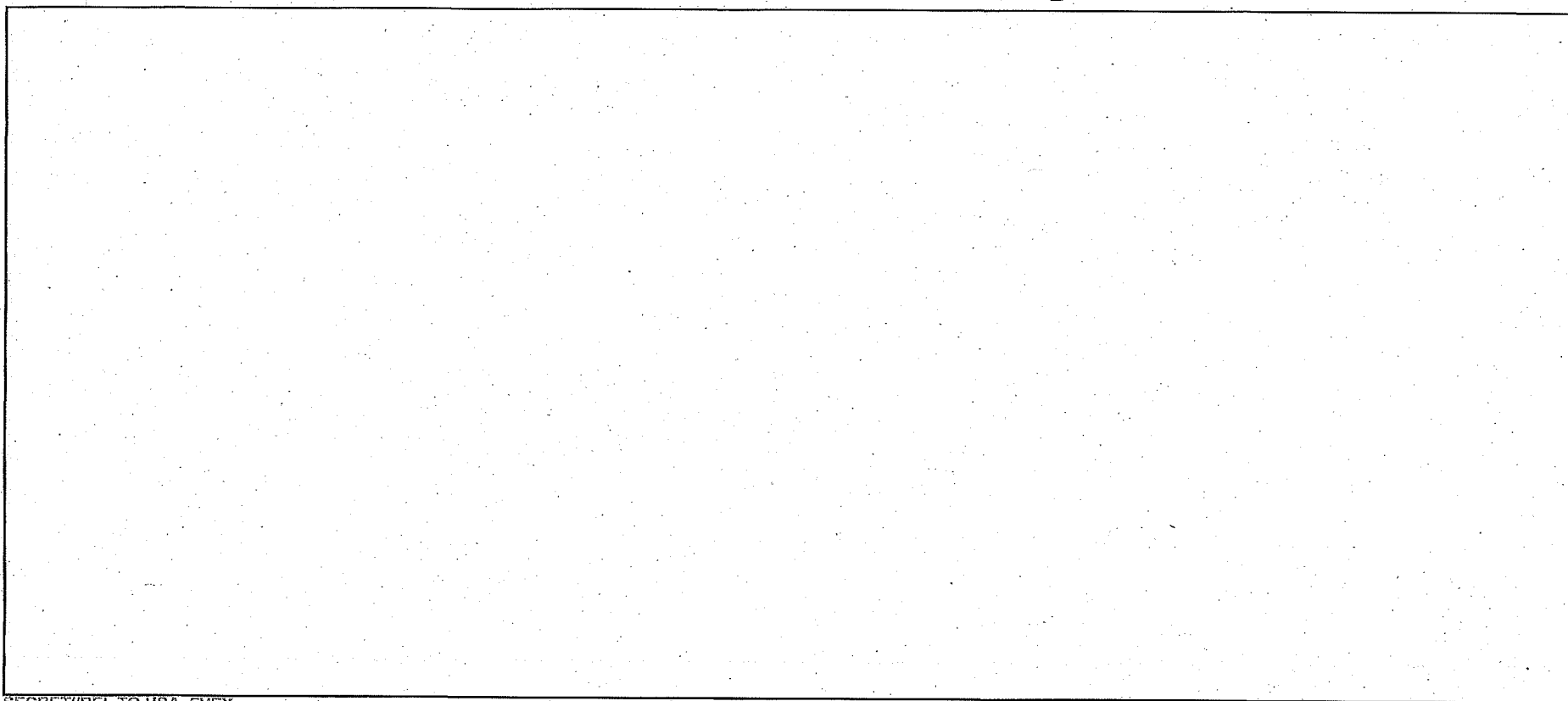


CNMF Task Force Structure





Cyber National Mission Force Threats, Roles, and Coordinating Authorities



~~SECRET//NOFORN TO USA, EYES~~

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

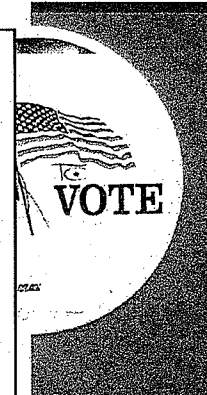
(b) (1) Sec. 1.4(a)

(b) (3) 50 U.S.C. §3605



CNMF

Defense of Elections

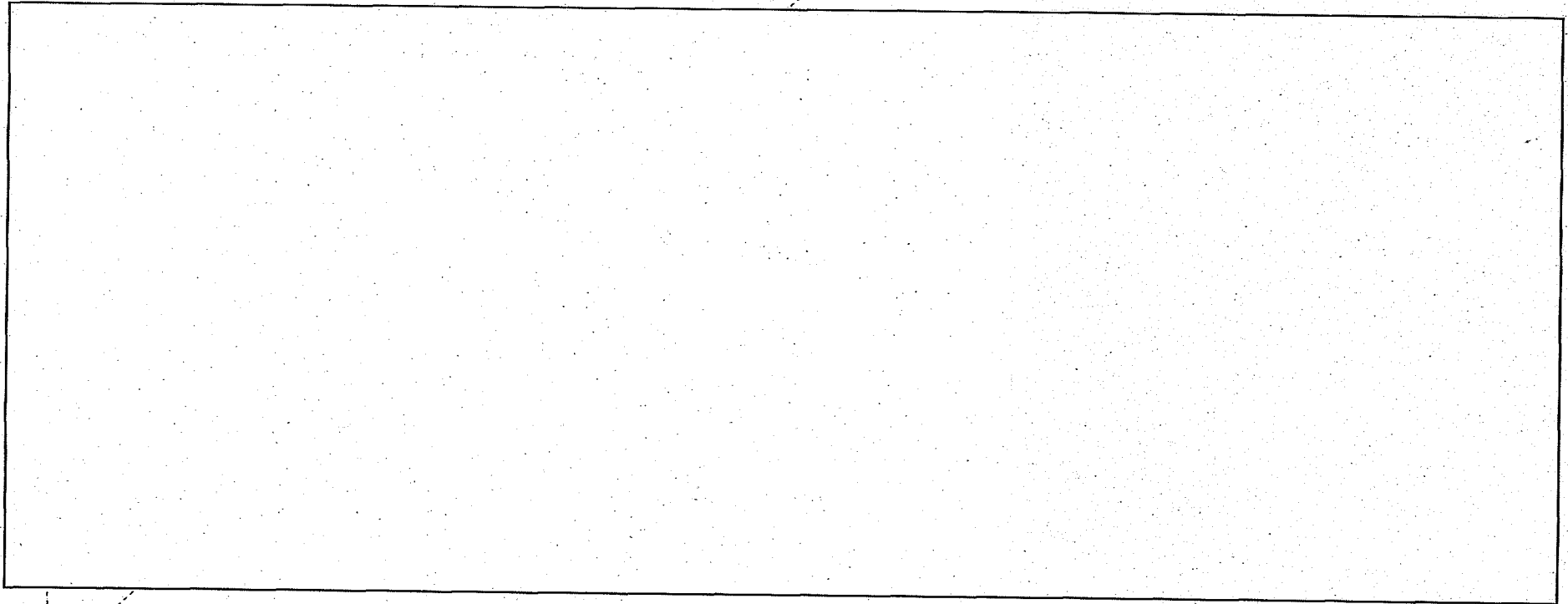


Problem Statement:

How do we develop **insight into Foreign Interference & Malign Influence** activity targeting the 2020 U.S. election in order to **assist DHS and FBI** in protecting the electoral process, while **imposing costs on aggressors** in cyberspace or elsewhere?



Exec Summary



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



(U) Proposed Operational Goals and Objectives

(U) Goals

- (~~S//REL TO USA, FVEY~~) [REDACTED]

(U) Objectives

Phase 0: Prepare

- (~~S//REL TO USA, FVEY~~) USCYBERCOM is postured **and** equipped to [REDACTED]

- (~~S//REL TO USA, FVEY~~) USCYBERCOM forces are postured to [REDACTED]

- (~~S//REL TO USA, FVEY~~) USCYBERCOM forces are postured and prepared to [REDACTED]

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



(U) Proposed Operational Goals and Objectives

Phase 1: Operate

- (~~S//REL TO USA, FVEY~~) [REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
[REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
[REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]

Phase 2: Assess

- (~~S//REL TO USA, FVEY~~) [REDACTED]
[REDACTED]
- (~~S//REL TO USA, FVEY~~) [REDACTED]
[REDACTED]

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

SECRET//REL TO USA, FVEY



JFHQ-C (AF) Profile Development

(b) (3) 50 U.S.C. §3605

- Project Profile

[Redacted]

- Fire Support Profile

[Redacted]

- Mission Profile

[Redacted]

- Mission Package

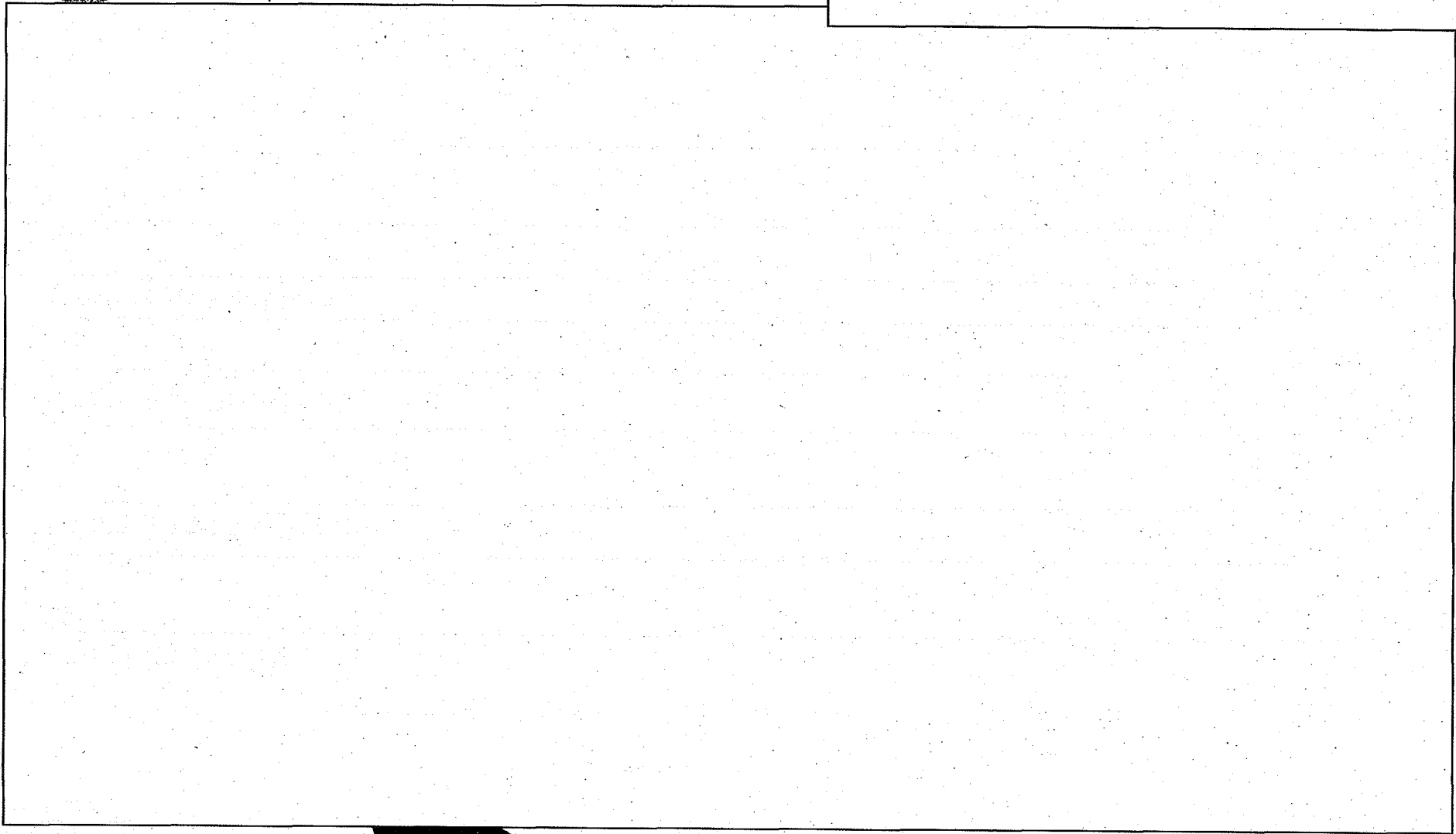
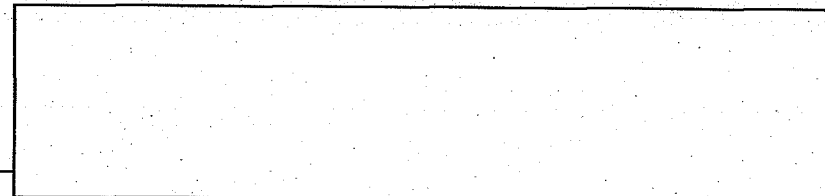
[Redacted]

[Redacted]

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



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



You are here

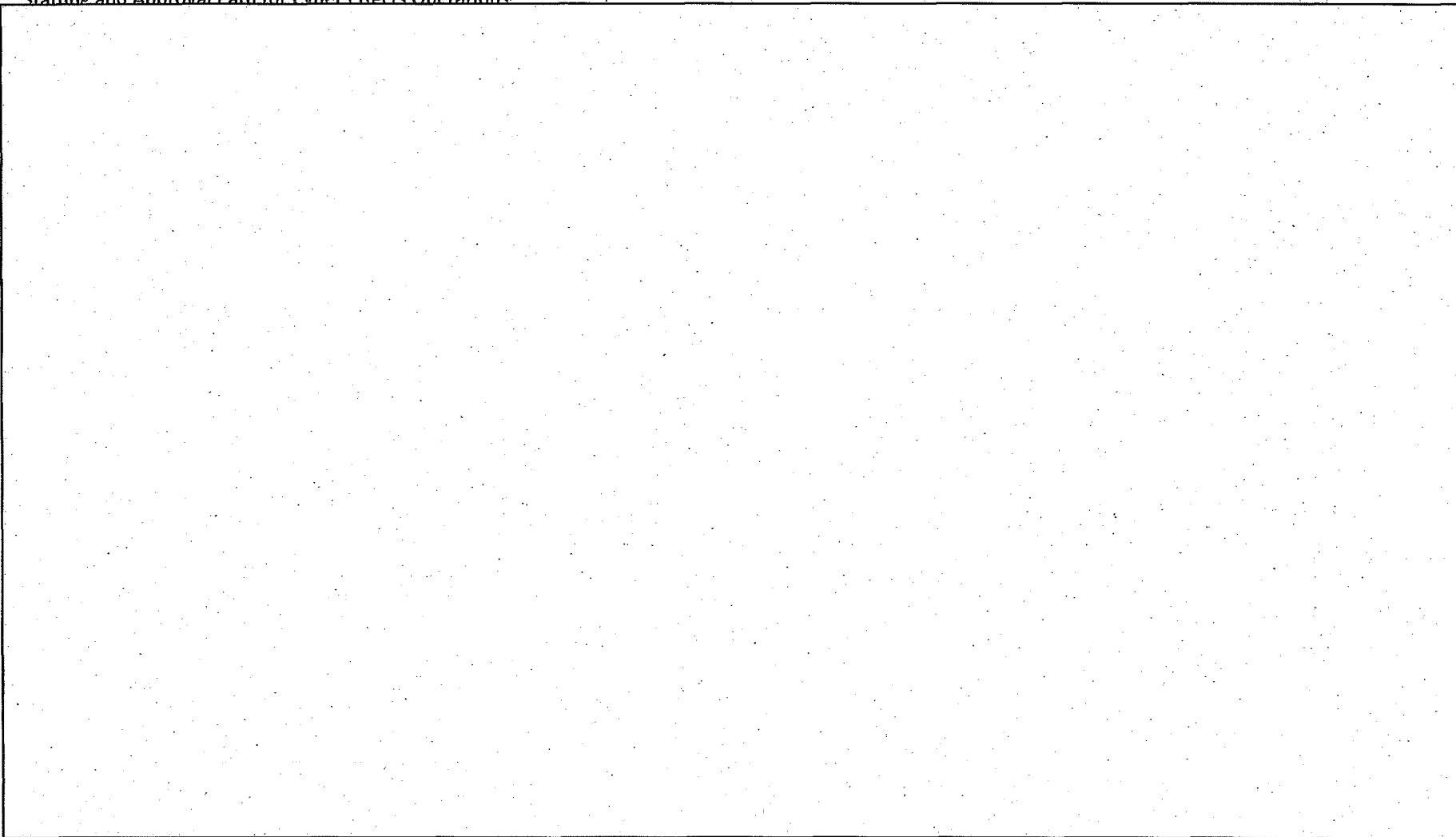


(b) (1) Sec. 1.4(a)

(b) (3) 50 U.S.C. §3605

Staffing and Approval Path for Cyber Effects Operations

SECRET

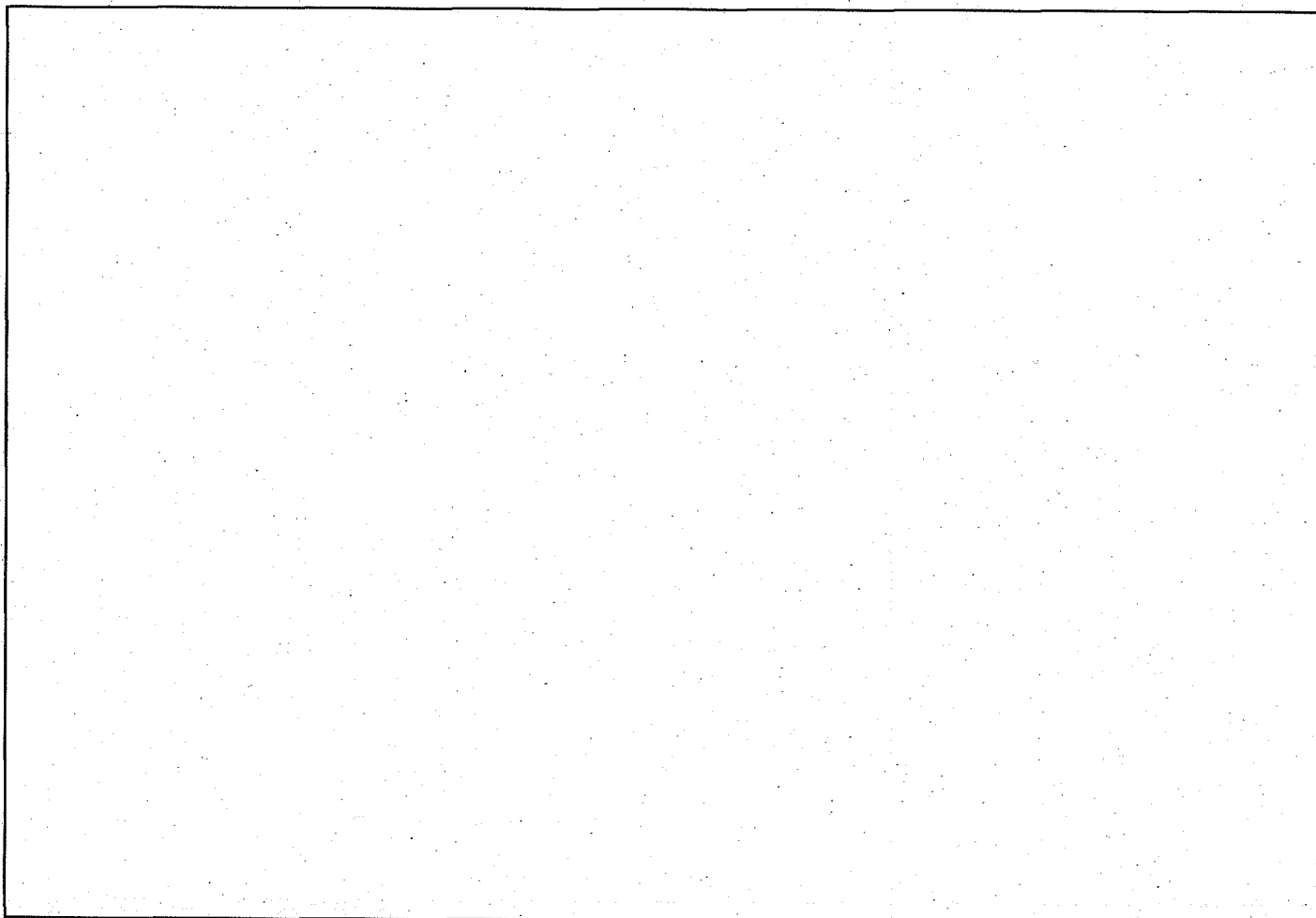


SECRET



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

SECRET//REL TO USA, FVEU



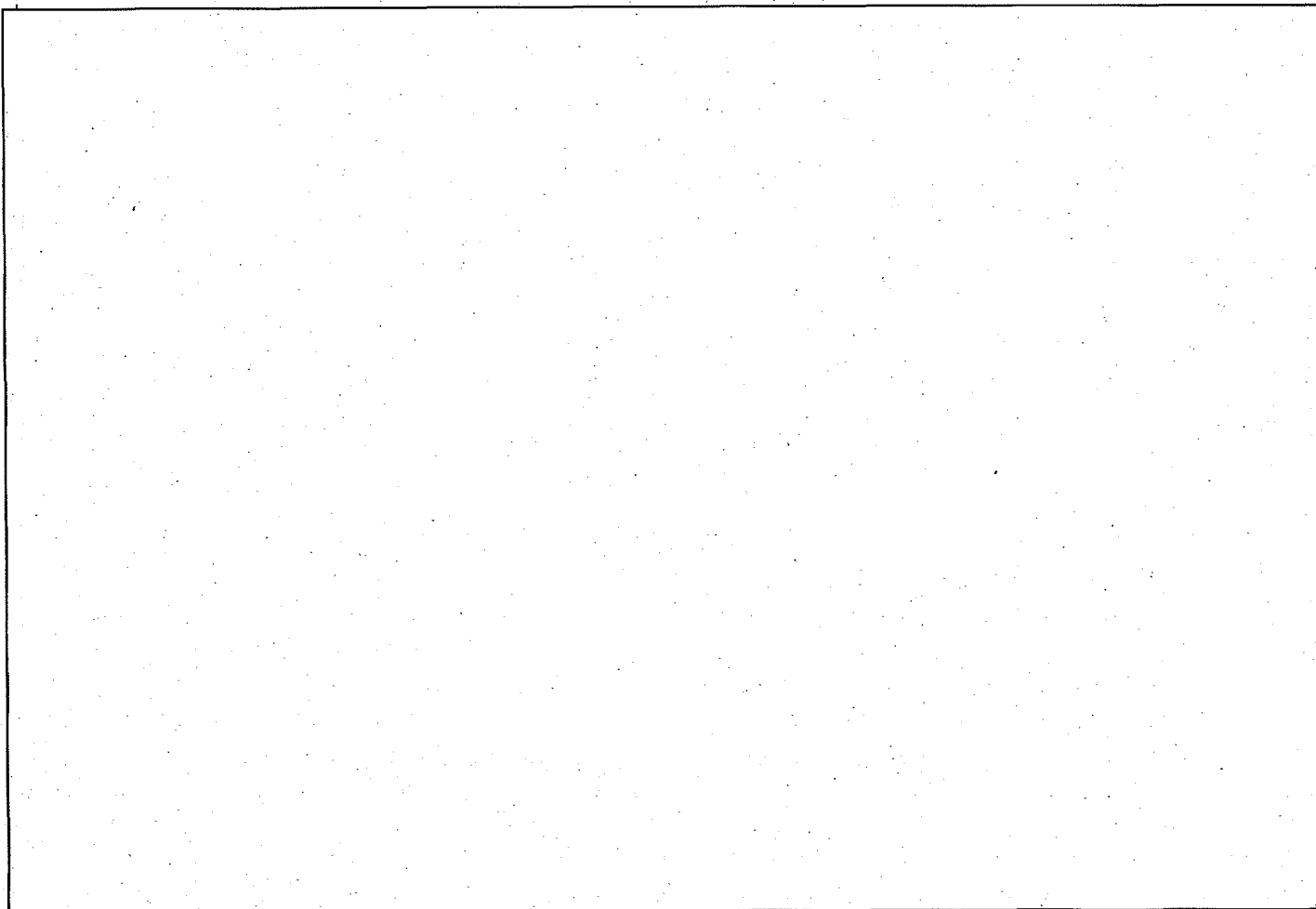
SECRET//REL TO USA, FVEU



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

(b) (3) 50 U.S.C. §3605

Mission Management

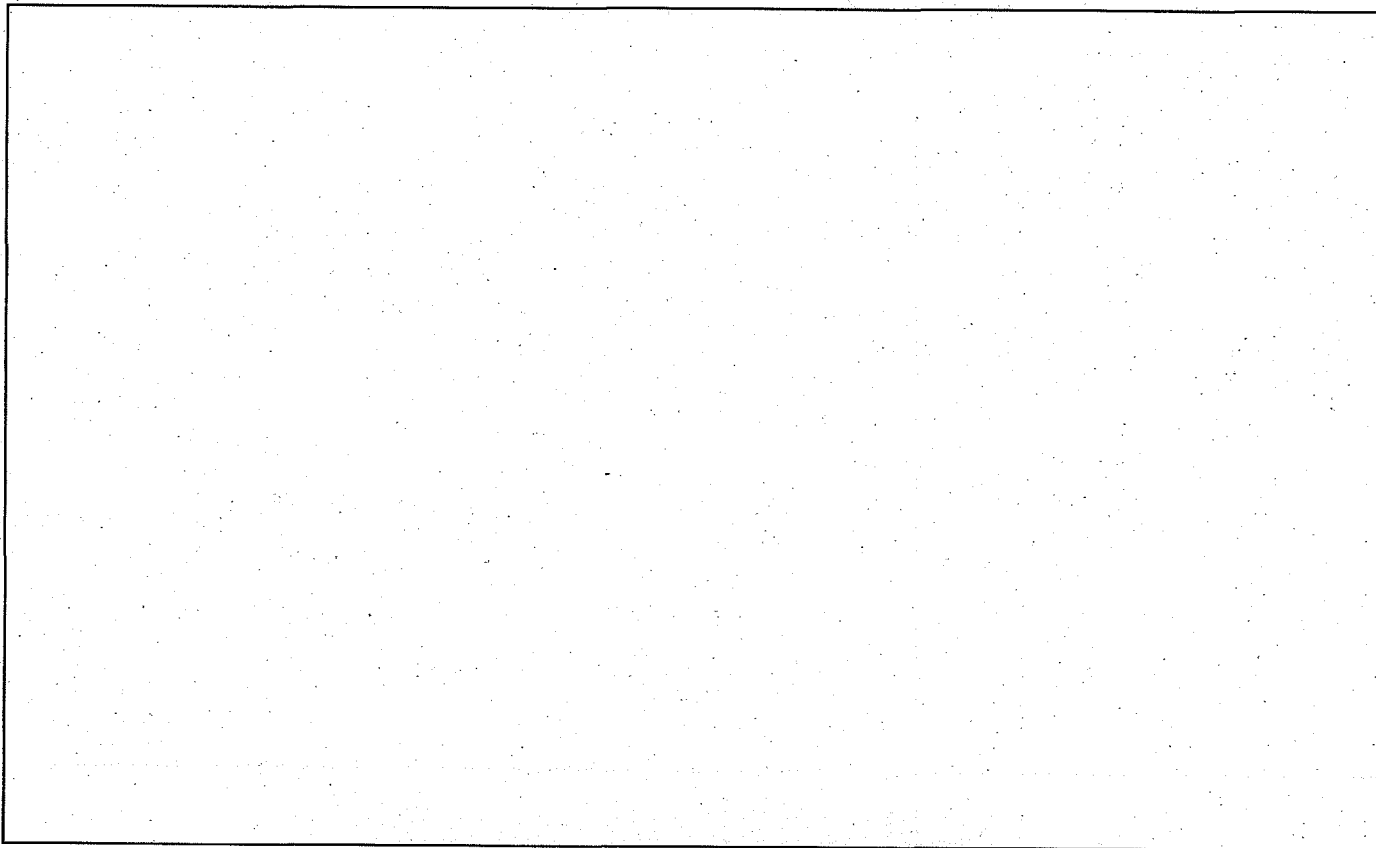




(b) (1) Sec. 1.4(a)

(b) (3) 50 U.S.C. §3605

Mission Management



CAO 27 DEC 18

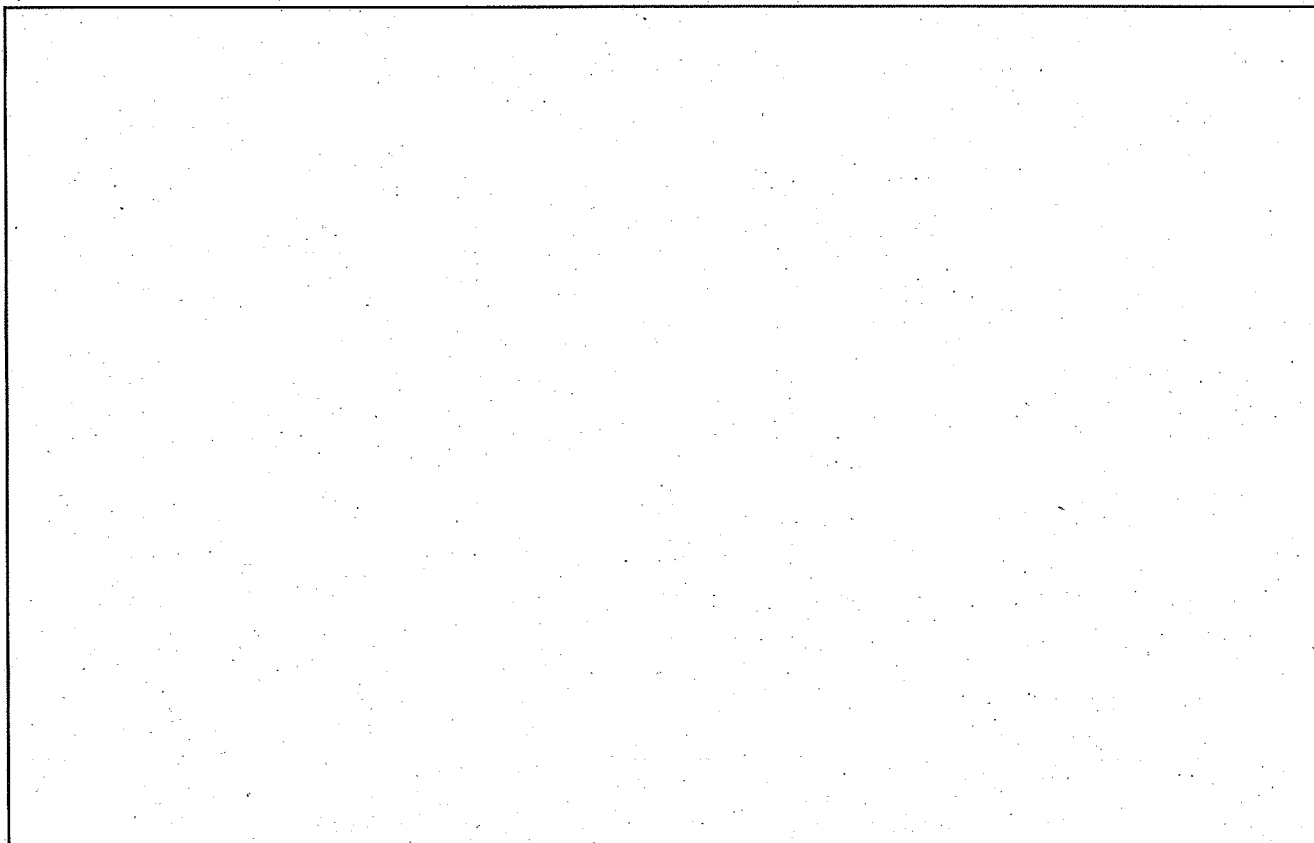


(b) (1) Sec. 1.4 (a) (c) (g)

(b) (3) 50 U.S.C. §3024 (i)

(b) (3) 50 U.S.C. §3605

Mission Management (Cont'd)



CAO 27 DEC38

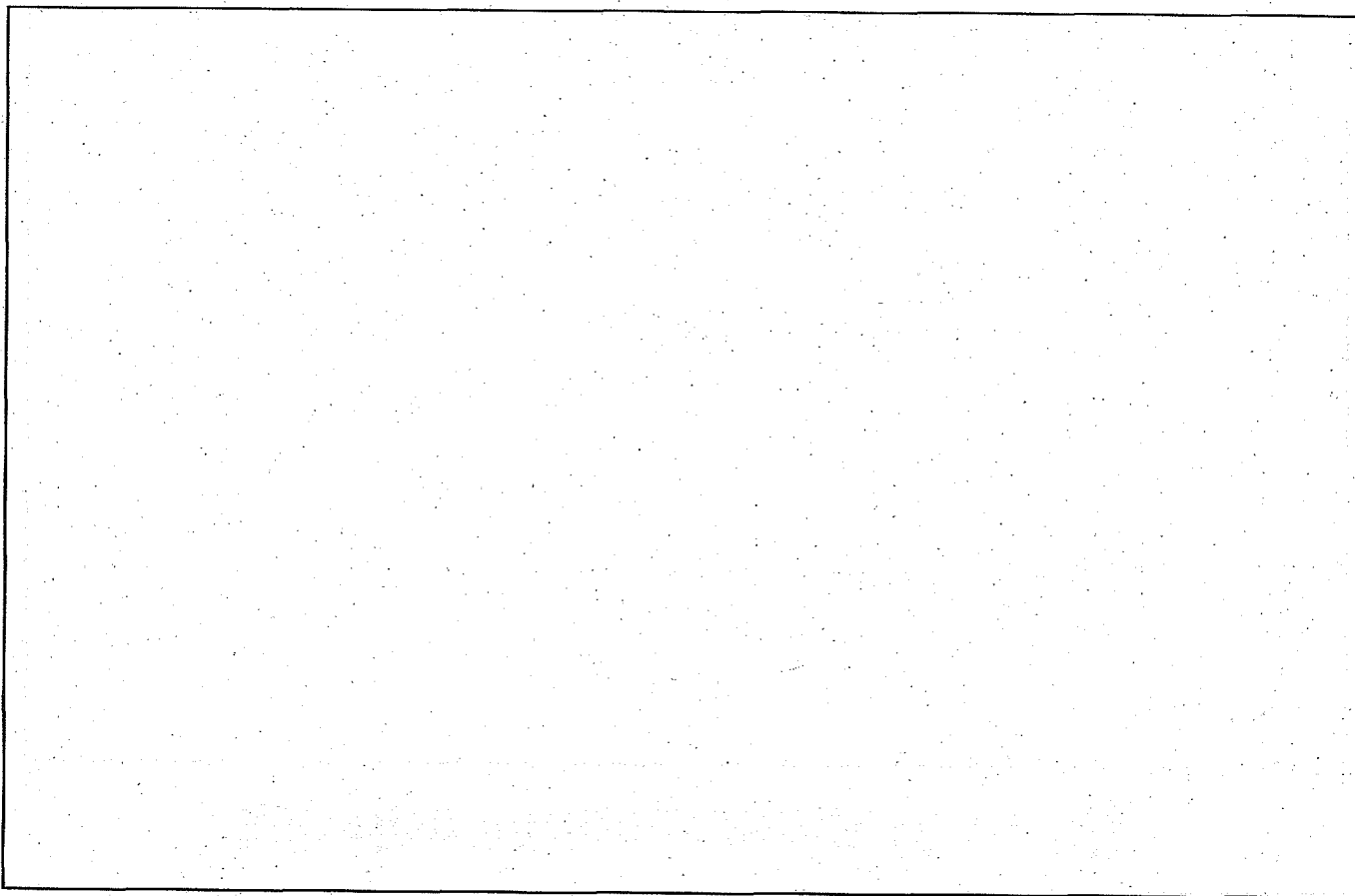


(b) (1) Sec. 1.4 (a) (c) (g)

(b) (3) 50 U.S.C. §3024(i)

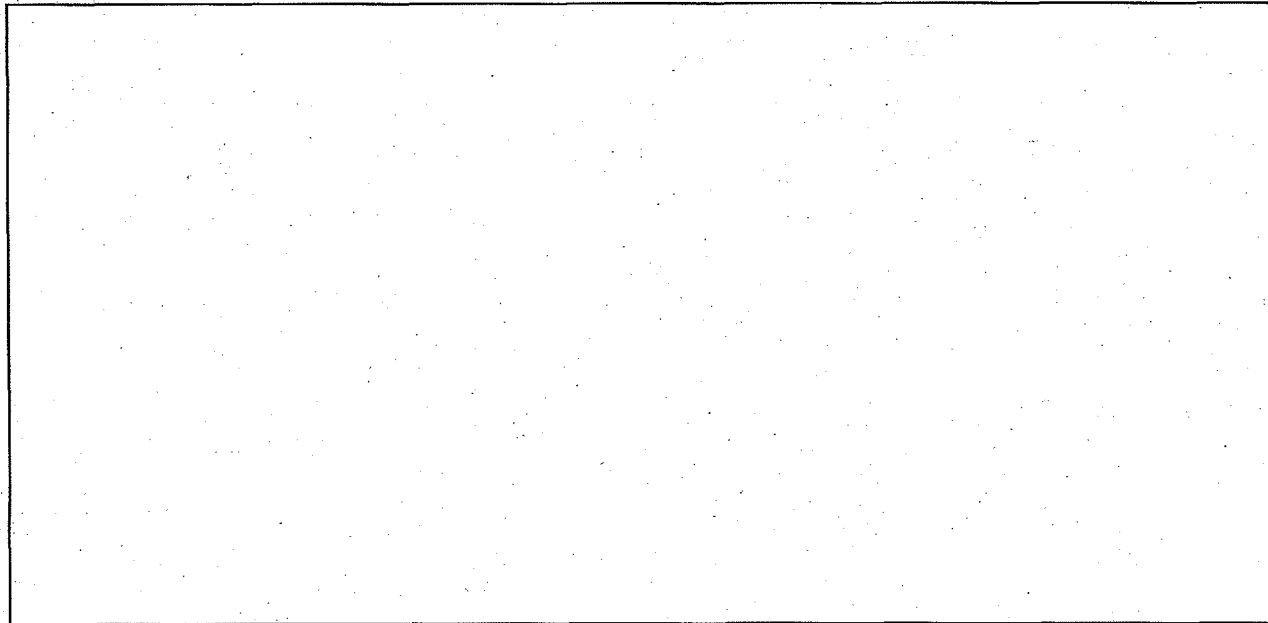
(b) (3) 50 U.S.C. §3605

Access Management





Infrastructure Management



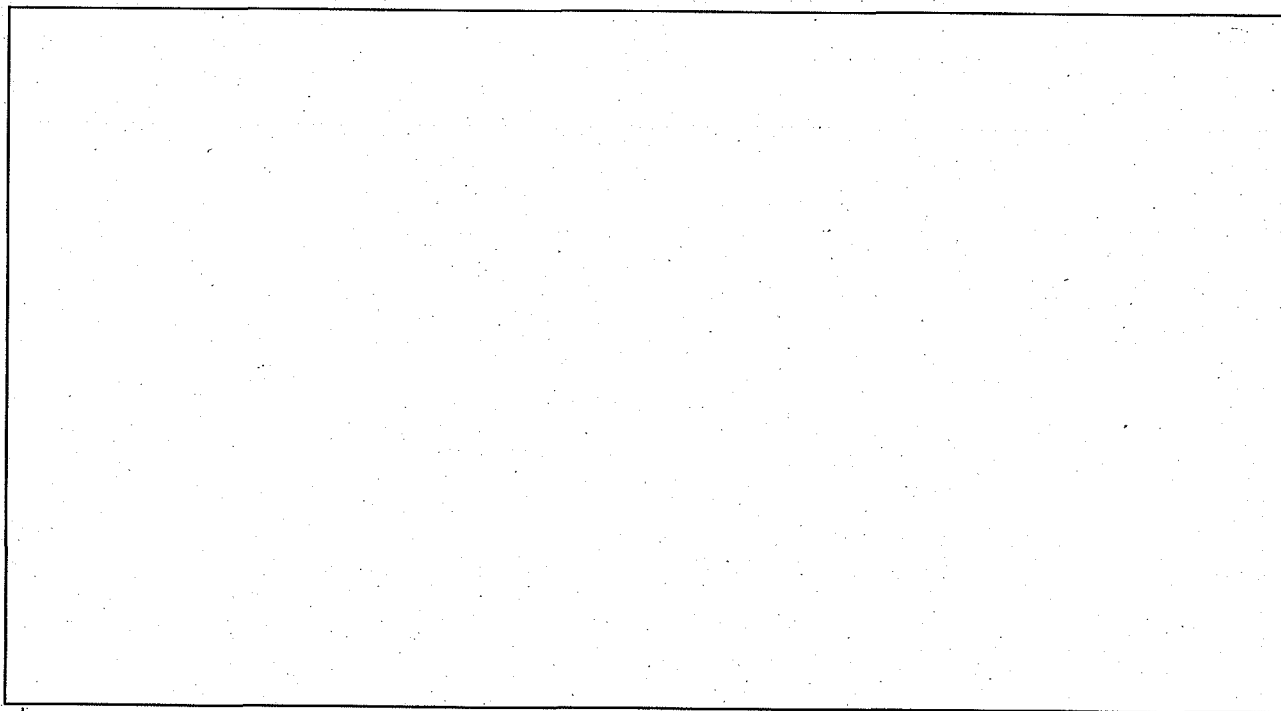
(b) (1) Sec. 1.4 (a)

(b) (3) 50 U.S.C. §3605

CAO 27 DEC 18



Capabilities Management



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

(b) (3) 50 U.S.C. §3605

CAC27 DEC 18



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

(b) (3) 50 U.S.C. §3605

Administrative

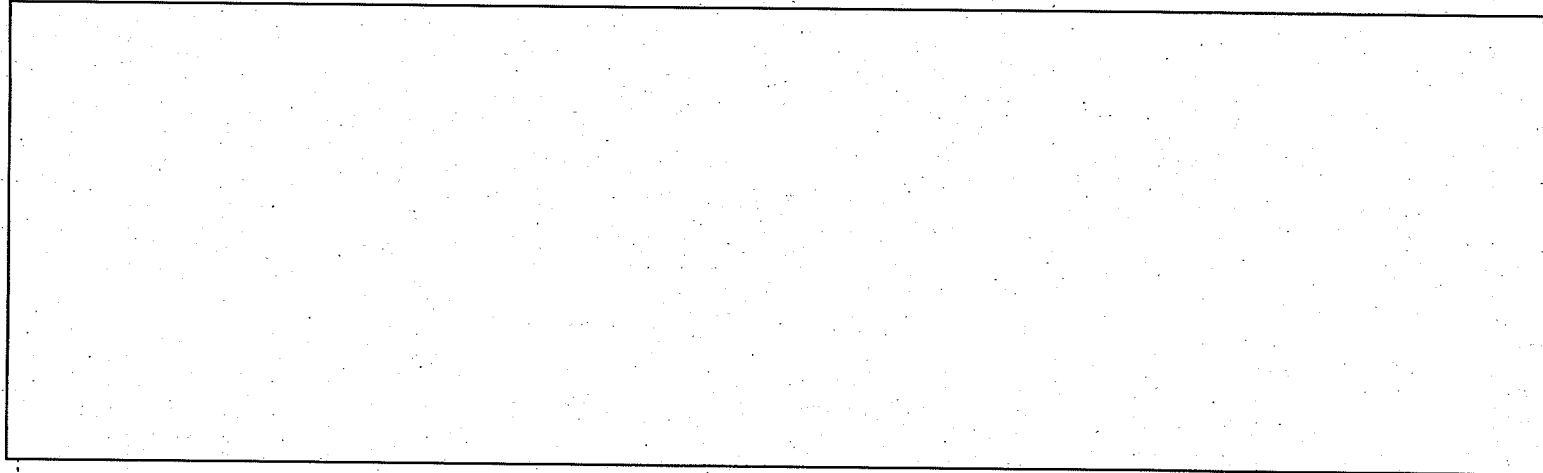




Back Up/Fail Safes

- Skype Rooms are Set up as required

-
-
-
-
-
-



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

(b) (3) 10 U.S.C. §130b

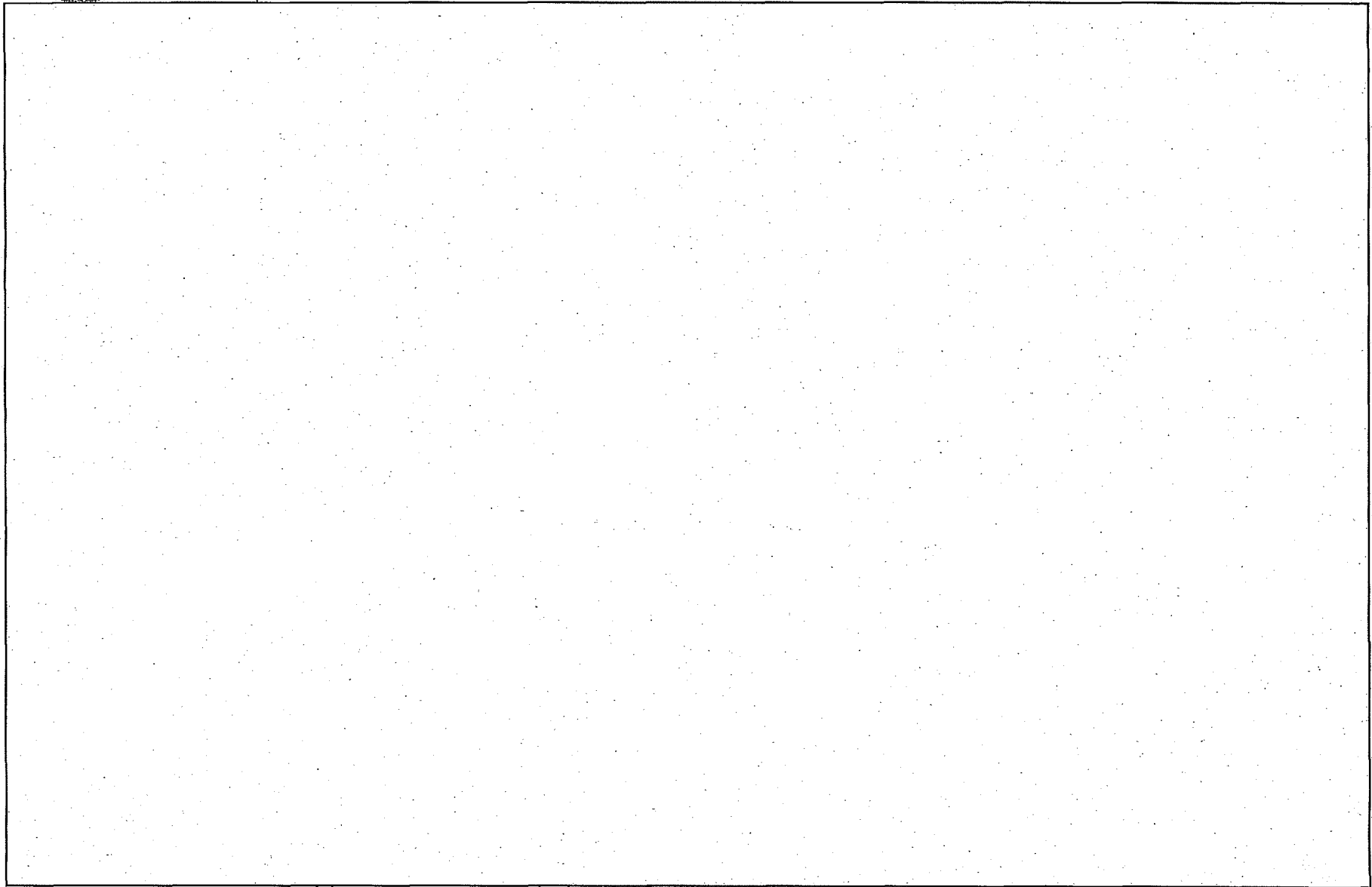
(b) (6)



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

(b) (3) 50 U.S.C. §3605

JFHQ-C (AF) Execution Tasks



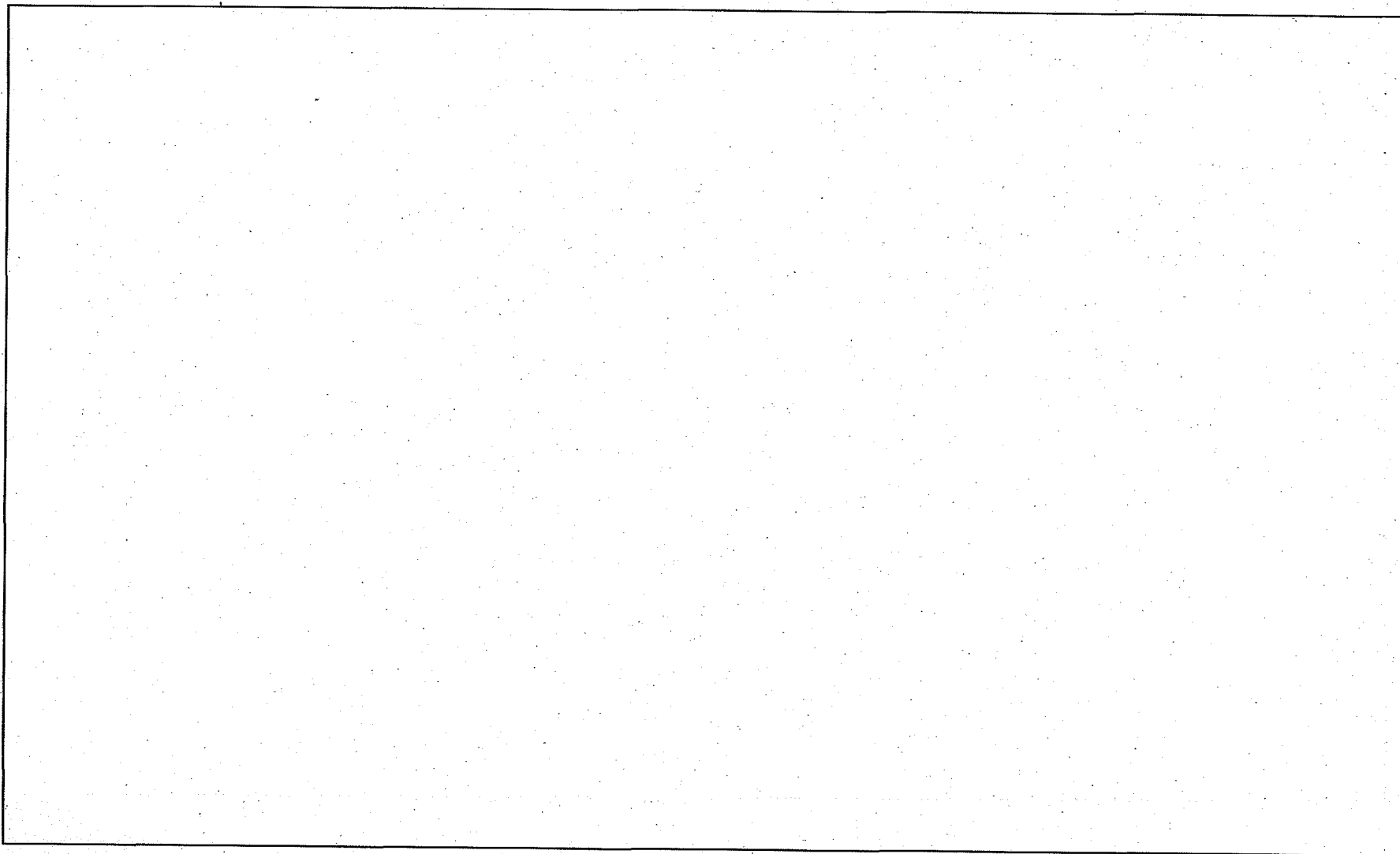
TOP SECRET//SI//REL TO USA, FVEY



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

(b) (3) 50 U.S.C. §3605

JFHQ-C (AF) Execution Tasks Cont.





Scenario Overviews

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



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

Scenario 1

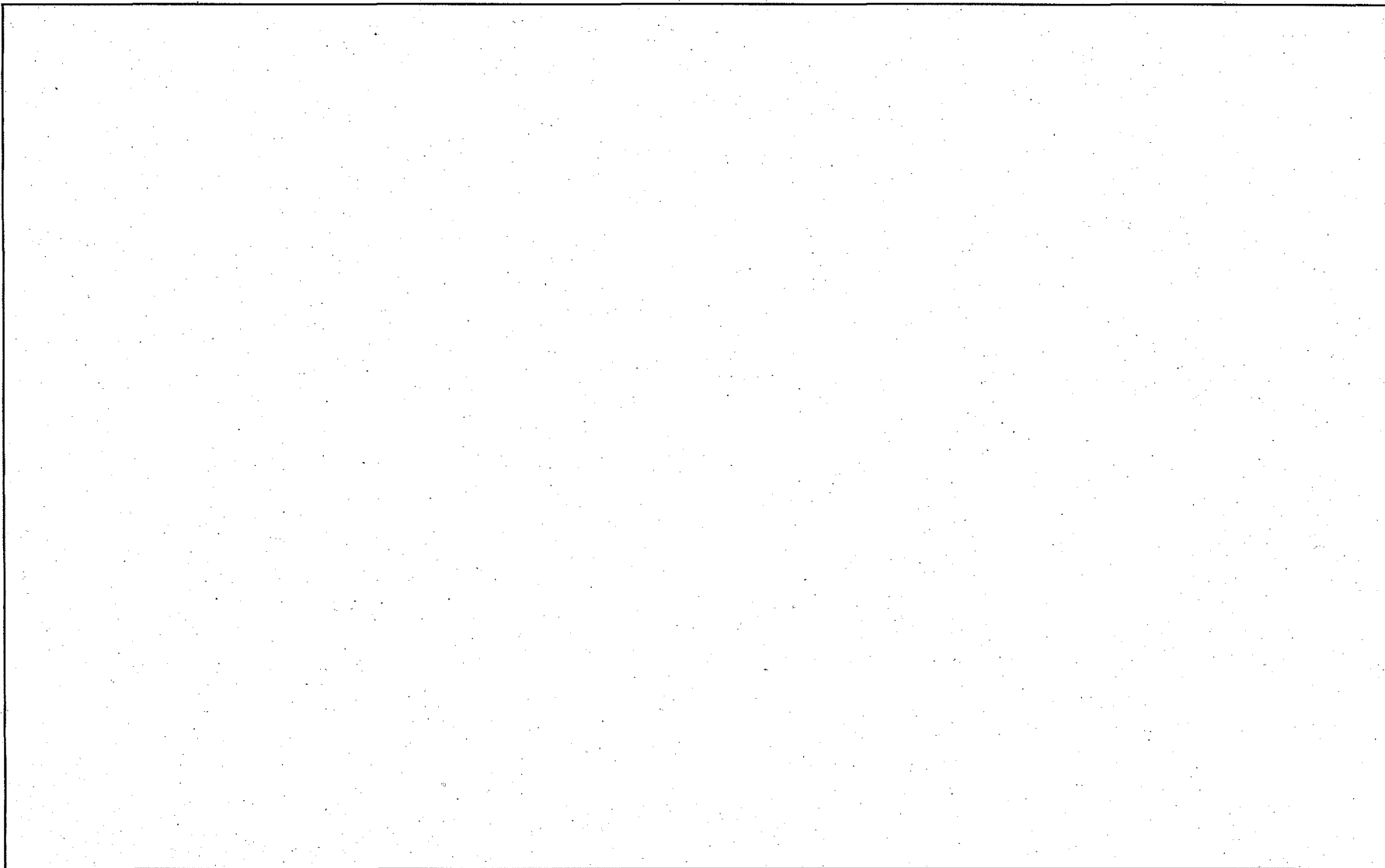
~~SECRET//REL TO USA, EYES~~

~~SECRET//REL TO USA, EYES~~



Scenario 1

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





Can an action happen?

ices?

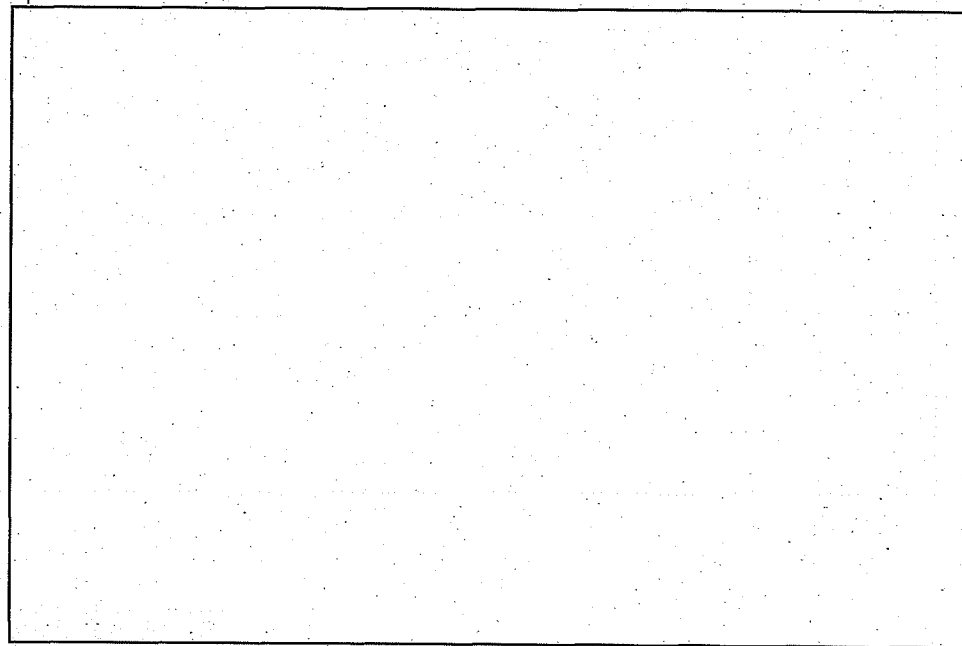
?

ored?

Scenario 1

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

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



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

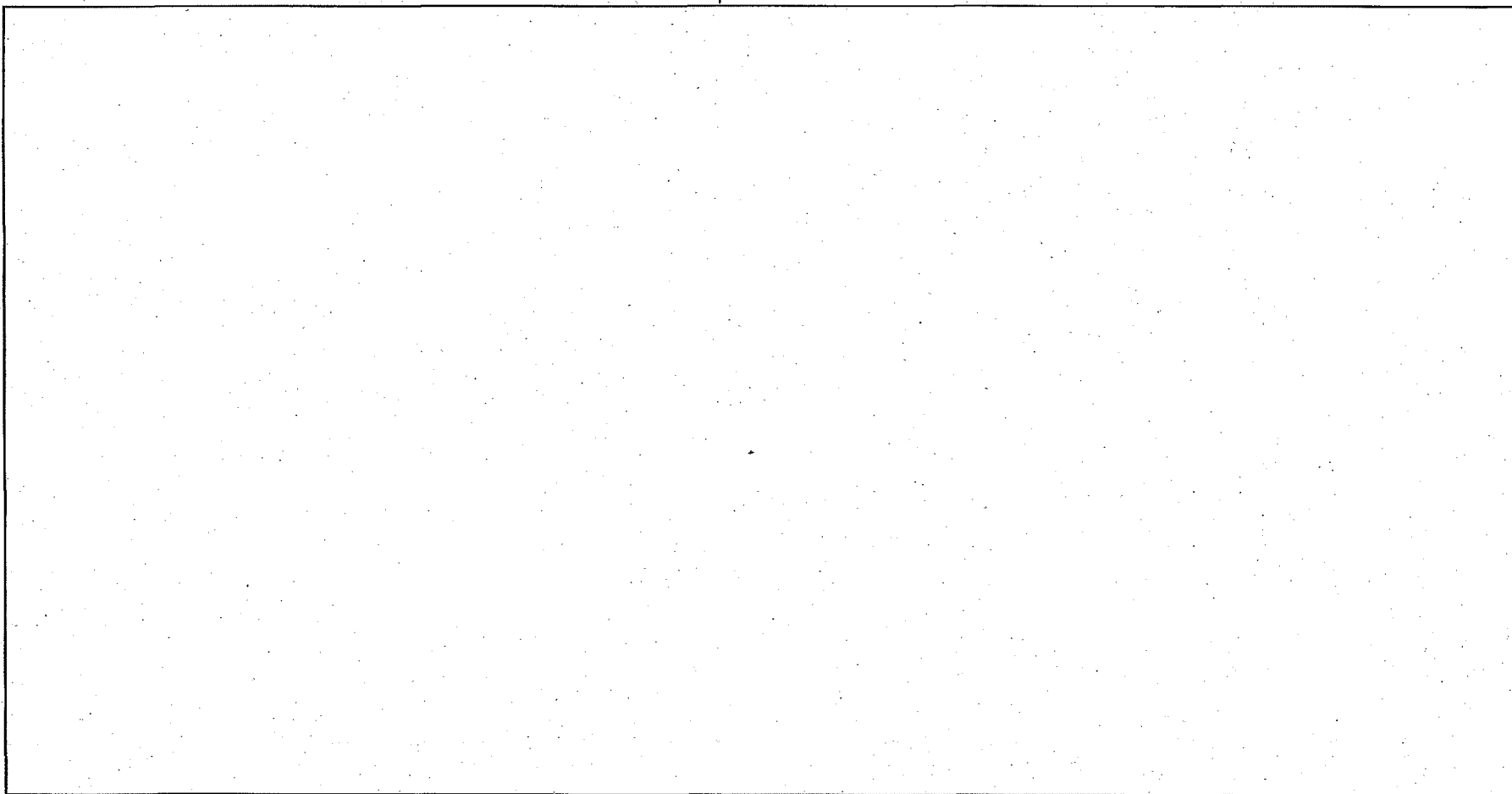


References

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

(b) (3) 50 U.S.C. §3605

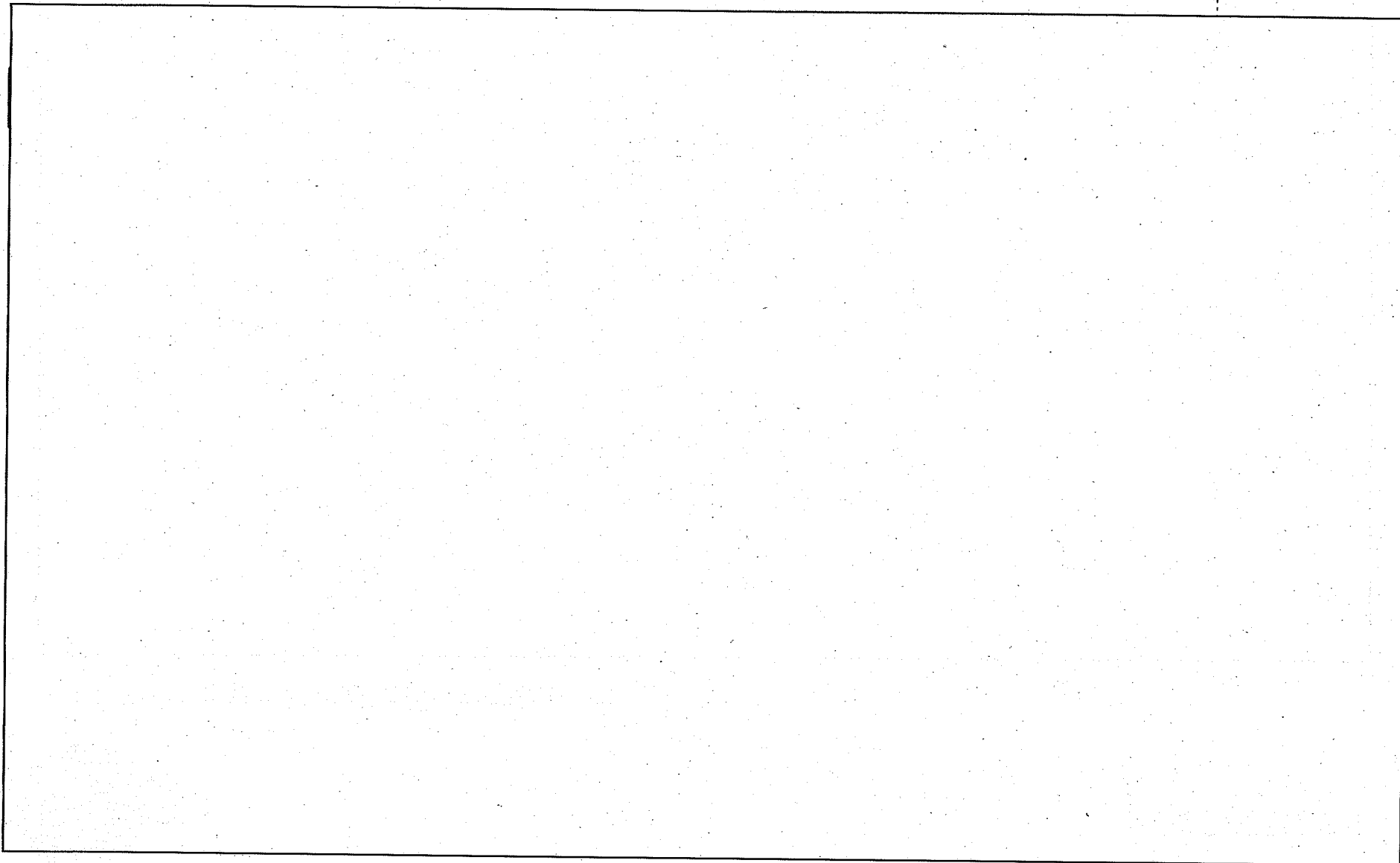
- All Reference Material is located at:





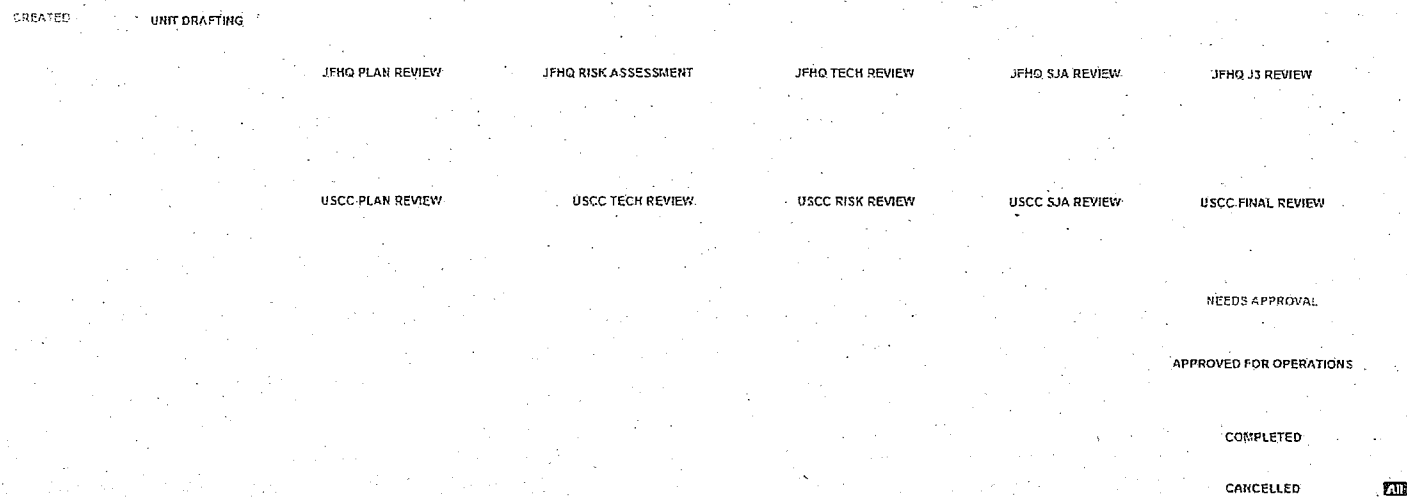
(U) USCYBERCOM CEO Planning and Approval

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





USCCMM: Review Workflow v2



Close



(U) Elections 2020 Battle Rhythm

UNCLASSIFIED//FOUO



Monday	Tuesday	Wednesday	Thursday	Friday

(b) (3) 50 U.S.C. §3605

UNCLASSIFIED//FOUO



**ELECTION
2020**

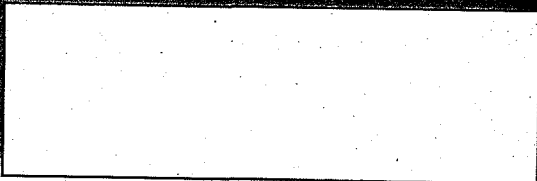
(TOP SECRET//SI//NOFORN)

(TOP SECRET//SI//NOFORN)

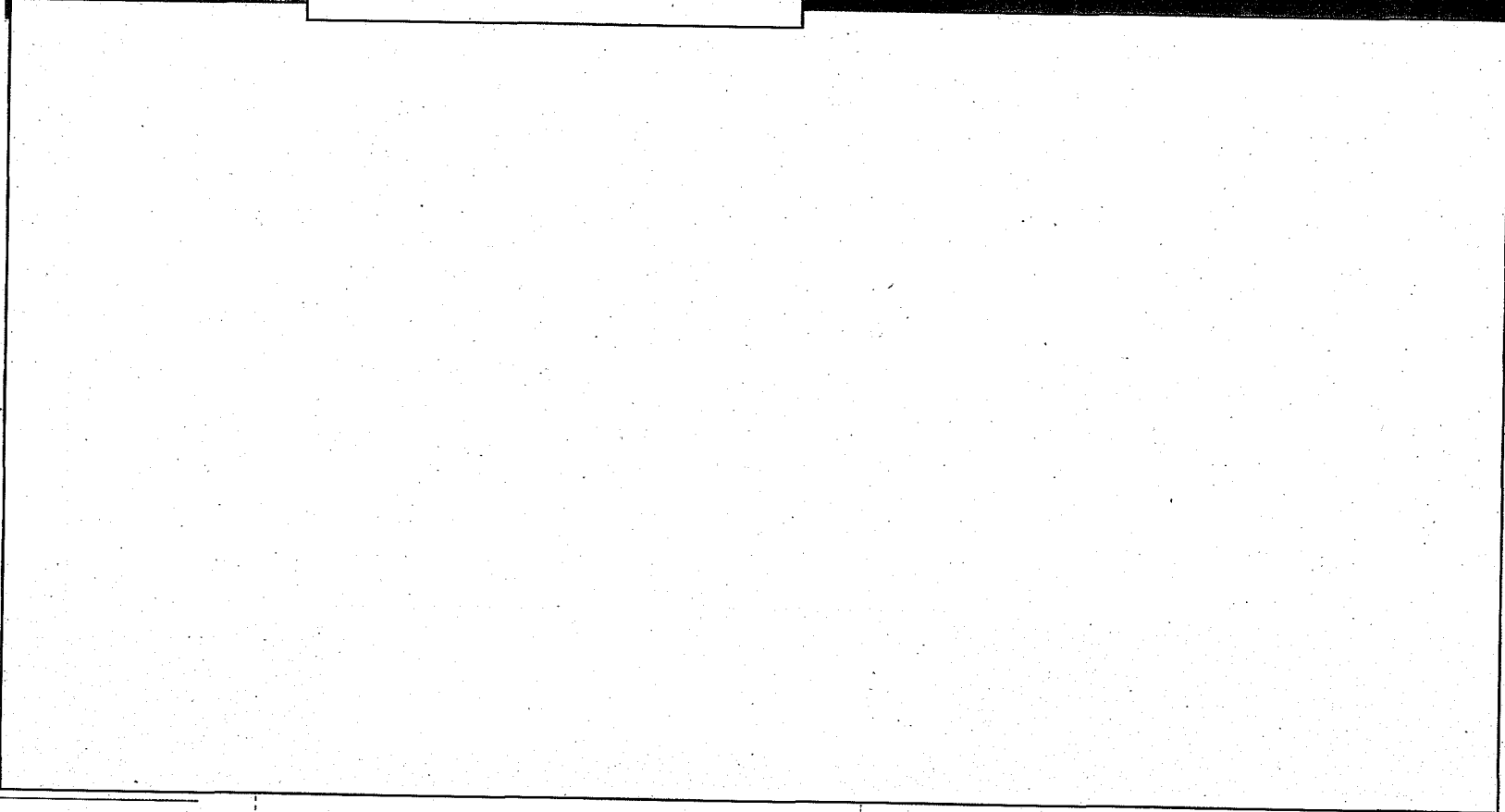
- (b) (1) Sec. 1.4(a) (c) (g)
- (b) (3) 18 U.S.C. §798
- (b) (3) 50 U.S.C. §3024(i)
- (b) (3) 50 U.S.C. §3605



**ELECTION
2020**



FOR OFFICIAL USE ONLY



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



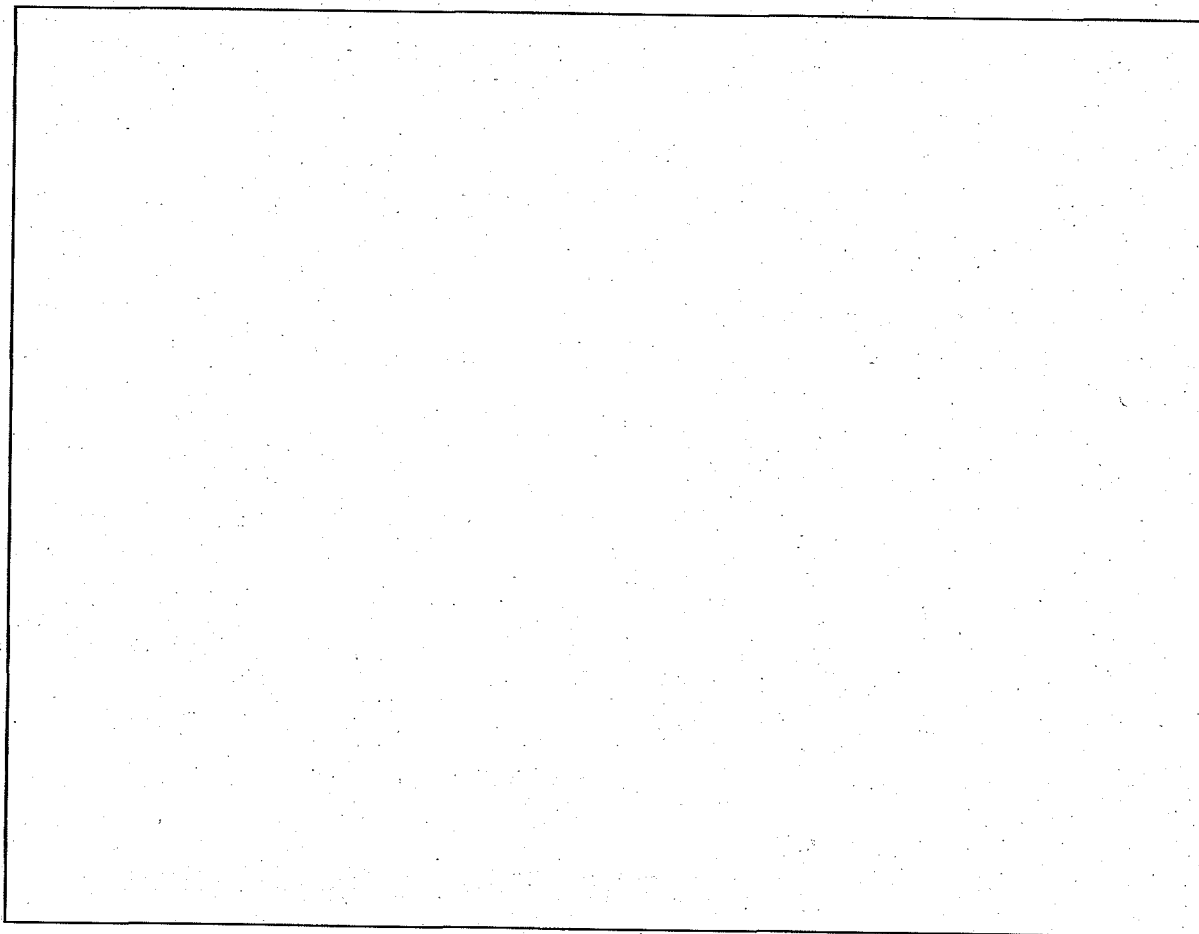
Outbrief

- TBD
 - Tentatively for 14 or 15 Nov



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

Cell Break Outs



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

(b) (3) 50 U.S.C. §3605

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