C05097682

~~SECRET~~

EXERCISE ELIGIBLE RECEIVER 97-1 (ER97-1) (U)

FINAL OBSERVATION REPORT (U)

~~December 1997 CLBV~~ ~~VADM George P. Steele, Jr.~~
~~Director, J7~~
~~CL REASON: 1.5(a)~~
~~DECL ON: X1~~

~~SECRET~~

C05097682

~~SECRET~~

Reply ZIP Code
20318-7000

MEMORANDUM FOR: Distribution List (limited)

SUBJECT: Final Observation Report for Exercise ELIGIBLE RECEIVER 97-1 (ER97-1)

1. (U) The Final Observation Report for ER97-1 is enclosed.

2. (U) Comments and questions concerning this report should be addressed to the J-7 JETD Project Officer, LTC (b)(6), at (b)(6)

3. (U) Without the enclosure, this letter is UNCLASSIFIED.

GEORGE F. CLOSE, JR.
Major General, USA
Director, Operational Plans and Interoperability

Enclosure

~~SECRET~~

C05097682

~~SECRET~~

TABLE OF CONTENTS

~~SECRET~~

~~SECRET~~

EXECUTIVE SUMMARY

(b)(1)

[redacted]

2. (U) Major Exercise Objectives

(b)(1)

[redacted]

3. (U) Overall Assessment. All ER97-1 objectives were achieved. A senior DOD official stated that ER97-1 was the most interesting, informative, and challenging exercise we have seen in a long, long time.

4. (U) UJTL Training. ER97-1 provided the opportunity for the Joint Staff to train on 26 Universal Joint Task List (UJTL) tasks. An assessment of the training is in Chapter XII.

5. (U) Observations and Recommendations. The findings and recommendations outlined below resulted from the analysis of the data and observations provided by players, controllers, and data collectors. A comprehensive listing of the actions taken to correct the deficiencies uncovered in ER97 is beyond the scope of this observation report. However, the Joint Staff Deputy Director for OperationsInformation Operations (J-39) will be identified as the lead office in developing this action plan in coordination with J-2 and J-6.

(b)(1)

d. (U) Recommendation. The DOD role in the protection of critical infrastructure, including the private sector, should be determined.

(b)(1)

f. (U) Recommendations

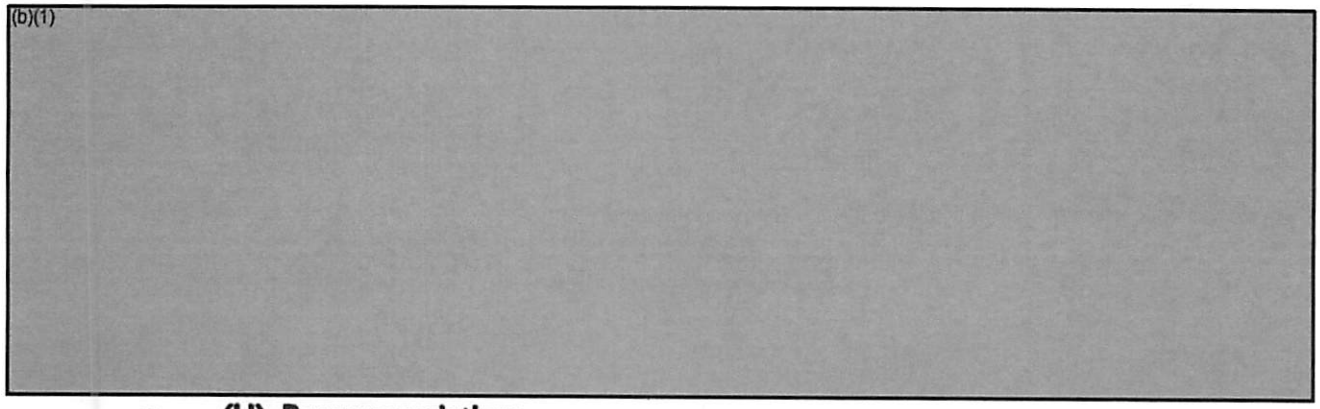
(b)(1)

(2) (U) The National Security Agency (NSA), in conjunction with DISA, should brief the commands on the lessons learned from system penetration attempts and successes in ER97-1.

(b)(1)

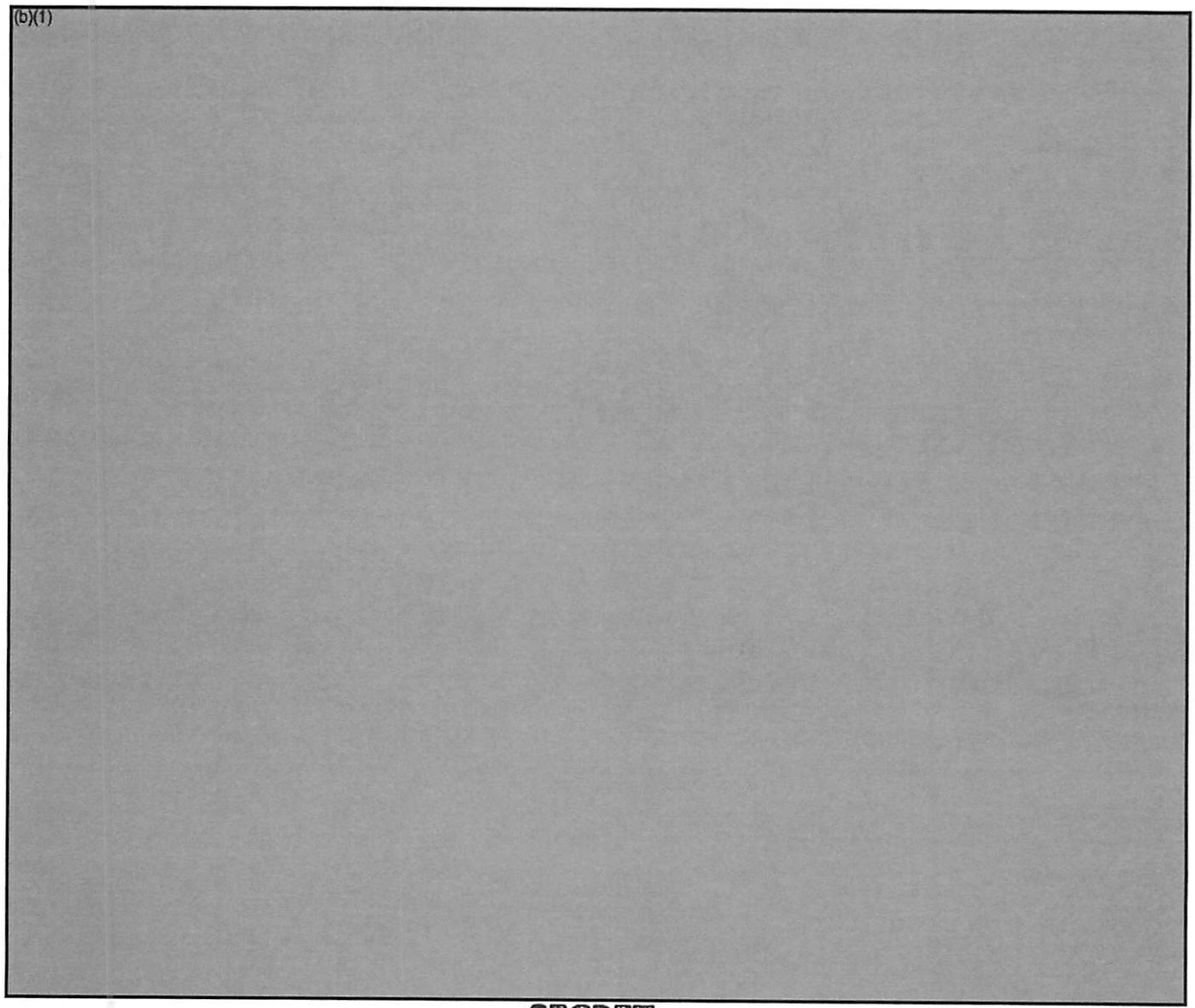
~~SECRET~~

(b)(1)



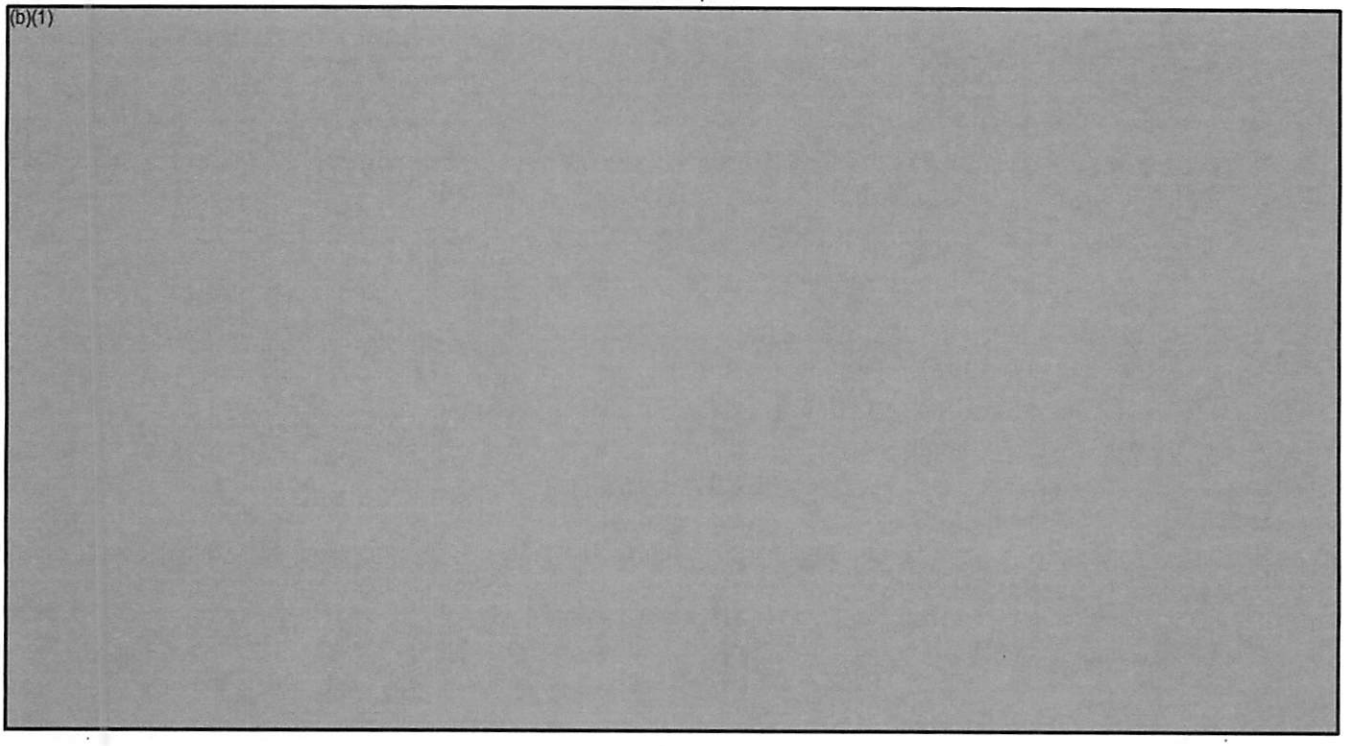
n. (U) **Recommendations**

(b)(1)



~~SECRET~~

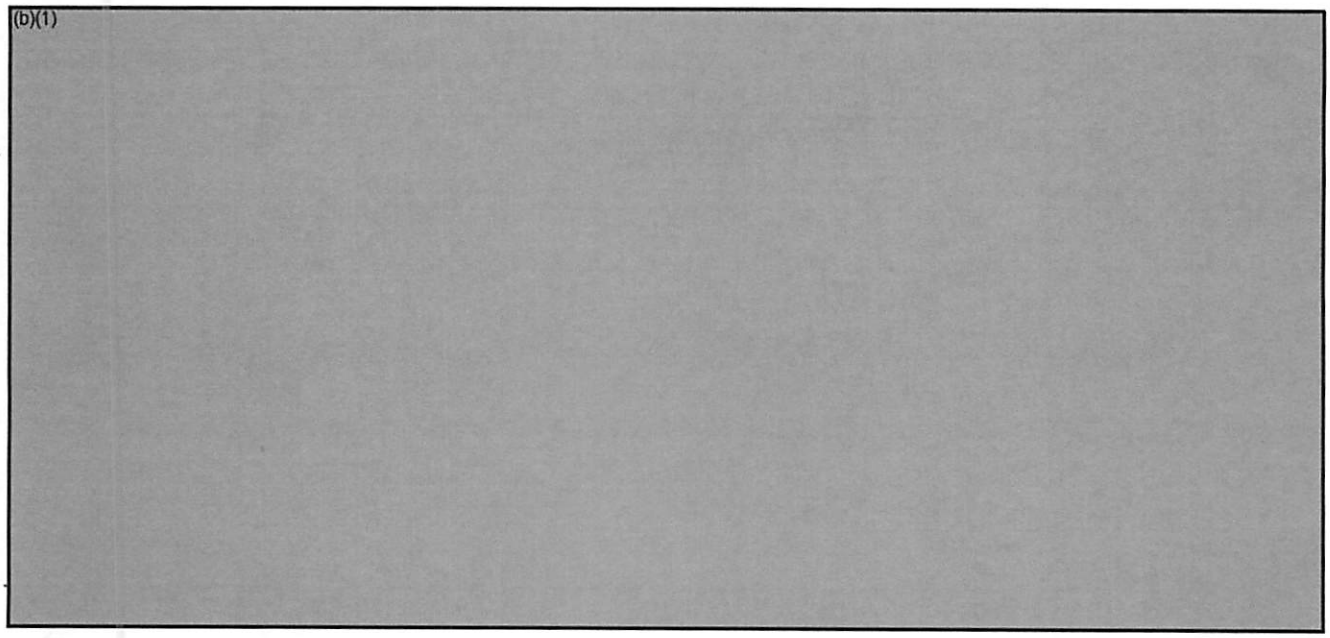
(b)(1)



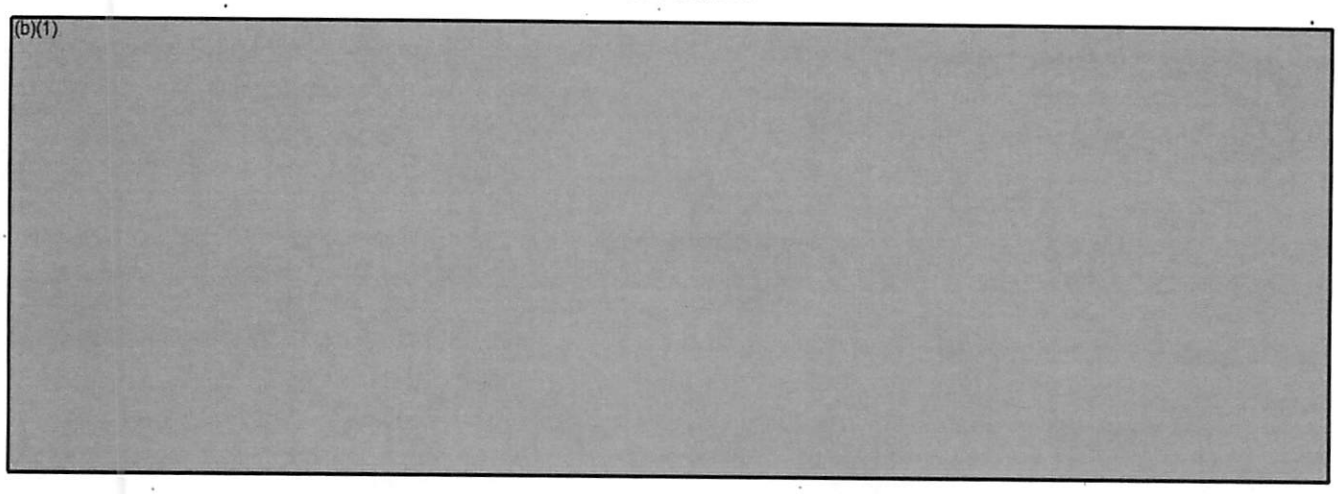
y. (U) Observation. The Joint Staff understood it needed the DISA Liaison Team but did not know how to use it.

z. (U) Recommendation. DISA and the Joint Staff should coordinate the role and duties of liaison teams and arrange adequate workspace, secure communications, and procedures to exchange information.

(b)(1)

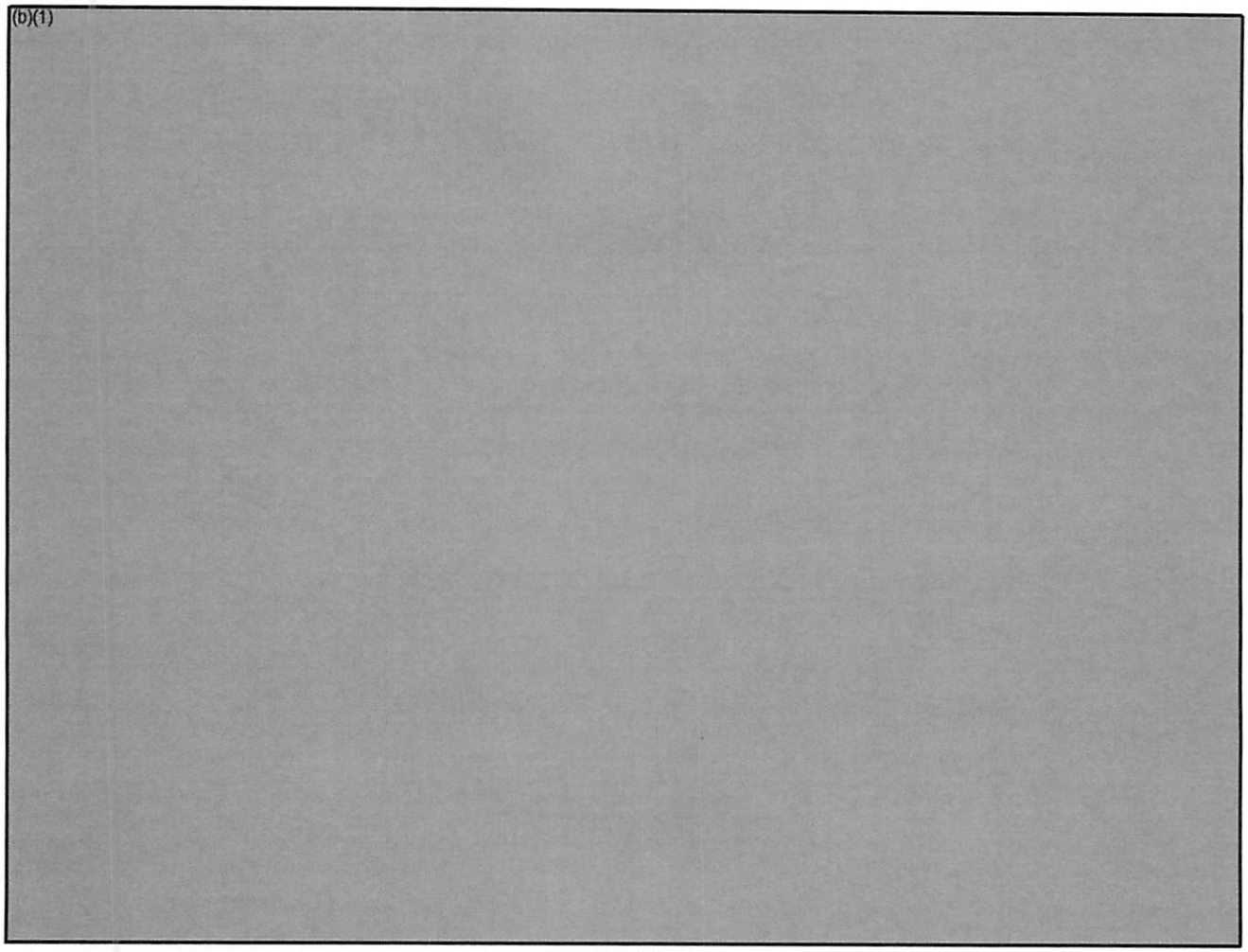


(b)(1)



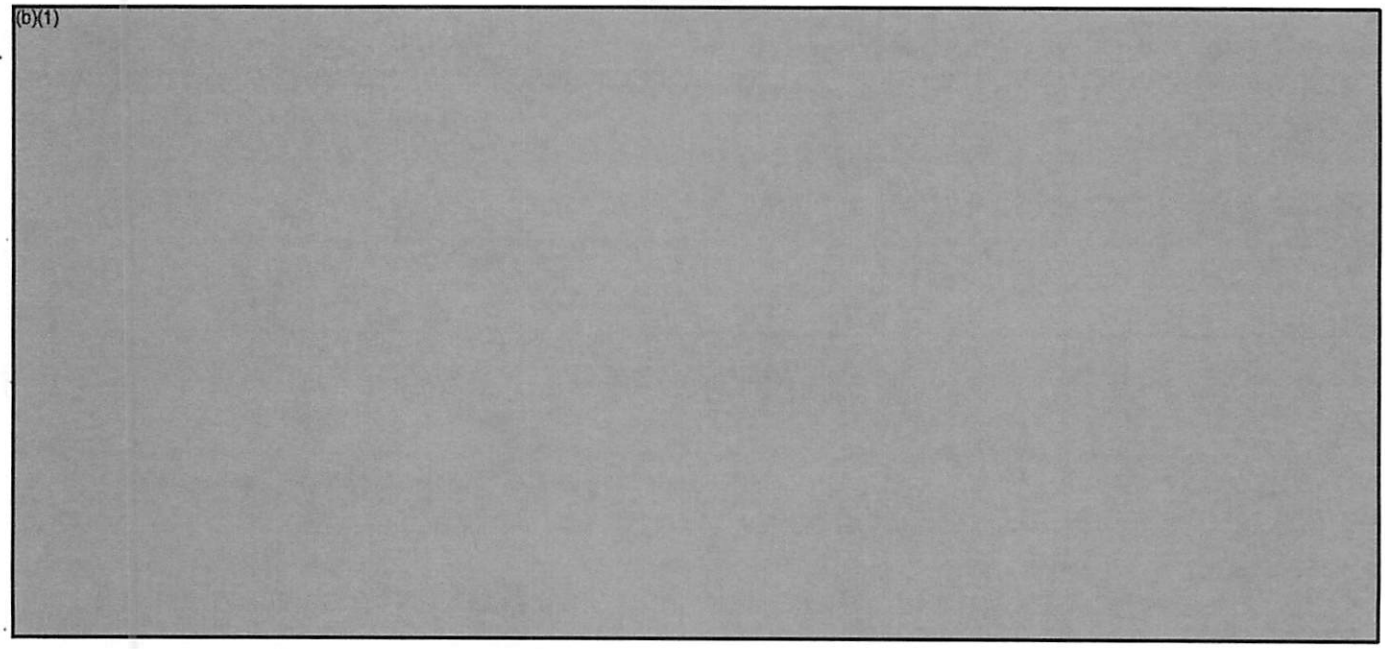
ai. (U) Observation. Even when they became aware that attacks on information systems were being widely reported, few organizations took additional defensive measures to preclude impact on their systems.

(b)(1)



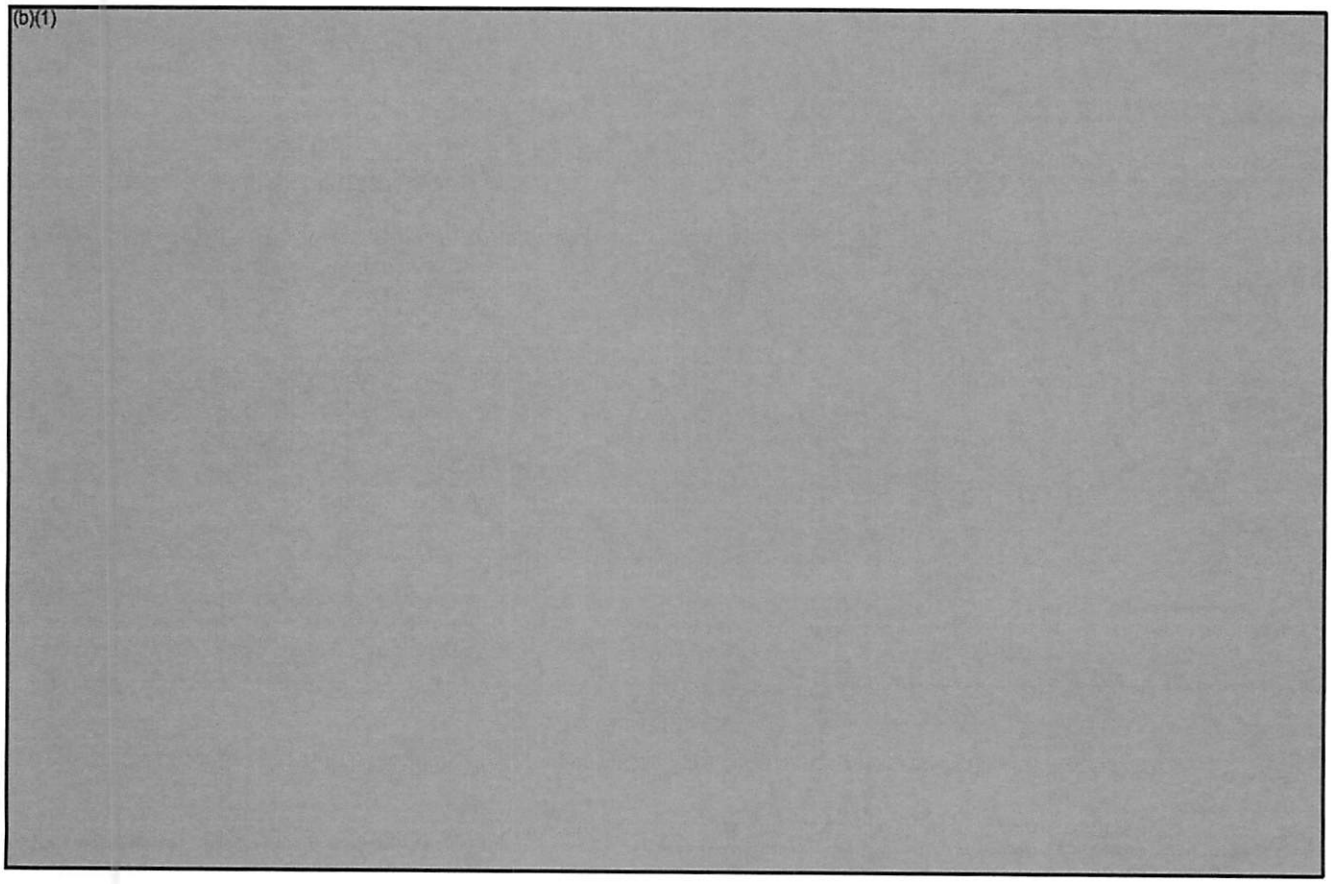
~~SECRET~~

(b)(1)



bh. (U) Recommendations

(b)(1)



~~SECRET~~

(b)(1)

bo. (U) Observation. The NMJIC experimented with various internal Intelligence Working Group configurations for the IO crisis.

(b)(1)

bq. (U) Observation. The lack of sufficient day-to-day IO intelligence and information reporting hampered Joint Staff efforts to provide intelligence fusion during a crisis.

br. (U) Recommendations

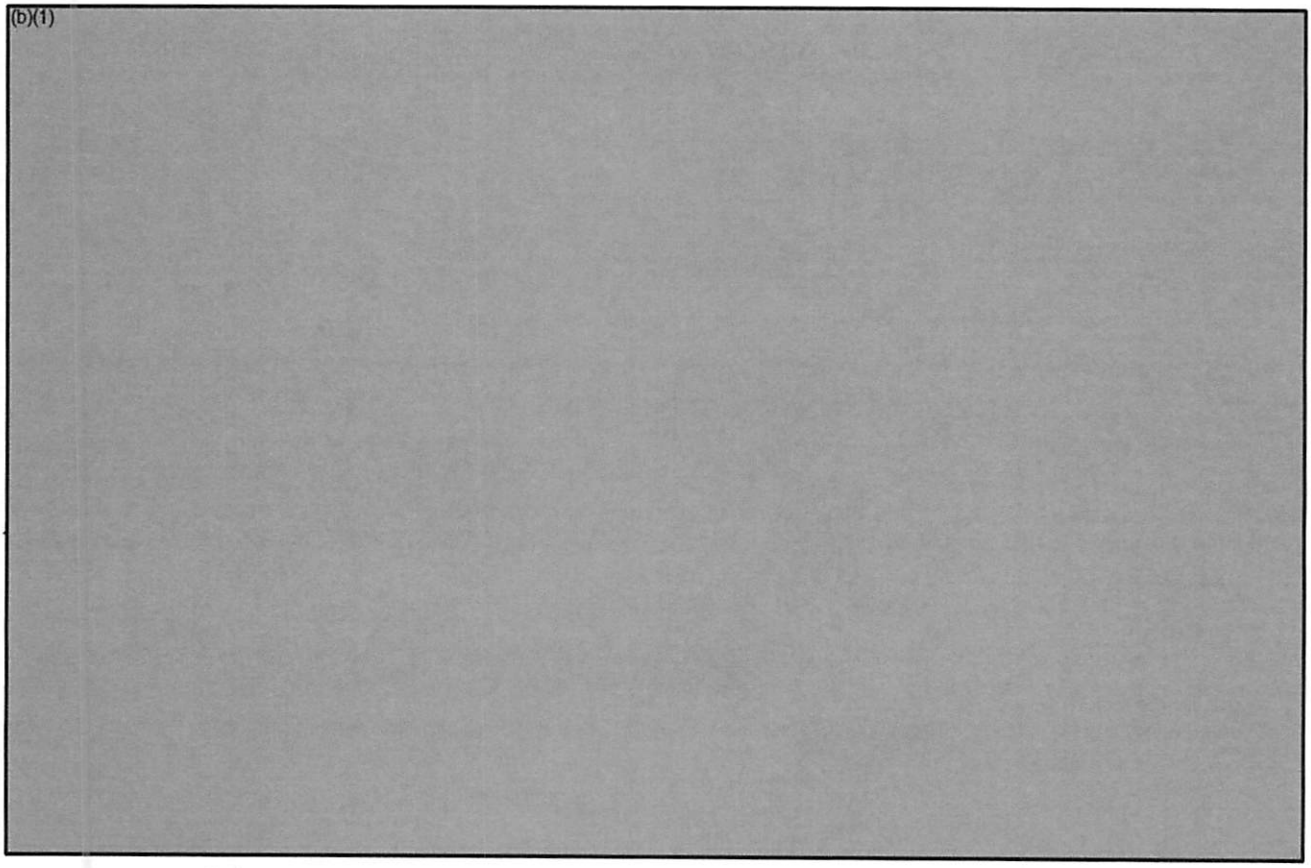
(b)(1)

bs. (U) Observation. During ER97-1 the NMJIC found the exchange of LNOs to be invaluable in interpreting information, facilitating the exchange of information, and providing technical advice.

(b)(1)

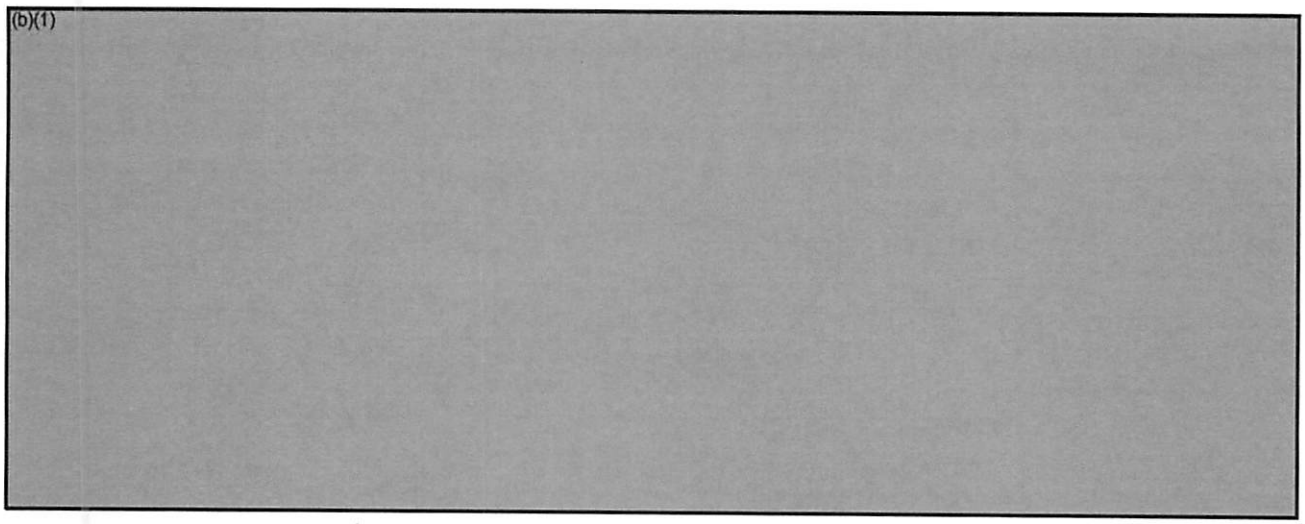
~~SECRET~~

(b)(1)



cp. (U) Recommendations

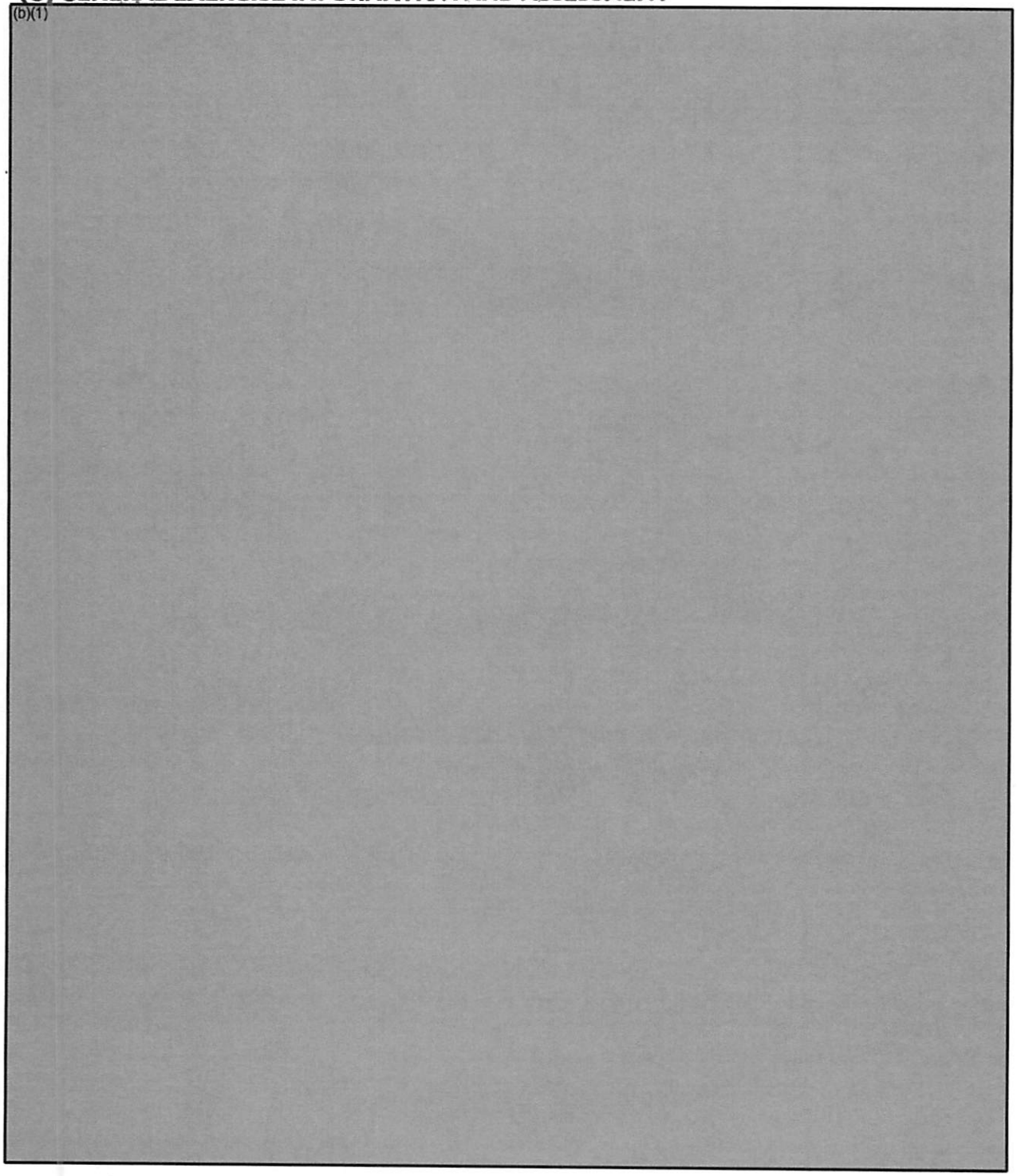
(b)(1)



~~SECRET~~

CHAPTER I
(U) GENERAL EXERCISE INFORMATION AND ASSESSMENT

(b)(1)



~~SECRET~~

3. (U) Major Exercise Objectives. Most of the major participants in ER97-1 established their respective exercise objectives (see Annex A) under the overarching NIEX objectives listed below:

(b)(1)

[redacted]

4. (U) Overall Assessment

a. (U) All ER97-1 objectives were achieved. A senior DOD official stated that ER97-1 was the most interesting, informative, and challenging exercise we have seen in a long, long time.

b. (U) Chapters II through X provide a detailed assessment of activities supporting the objectives. Other participants objectives were not assessed by the Joint Staff observation team.

5. (U) Exercise Design

(b)(1)

[redacted]

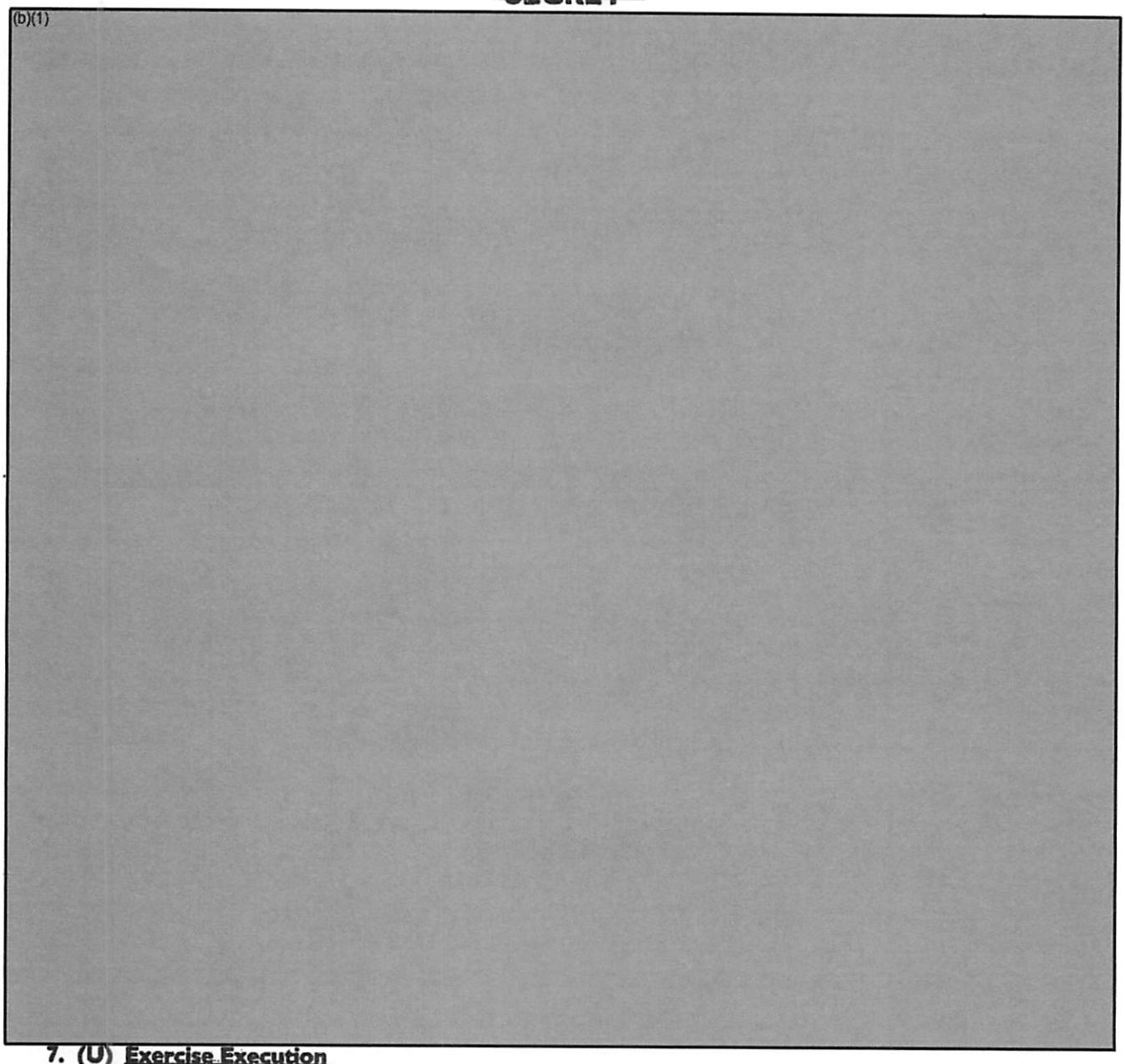
6. (U) Background Scenario. ER97-1 presented the participants with the following background scenario to set the stage for the start of the exercise on 9 June 1997.

(b)(1)

[redacted]

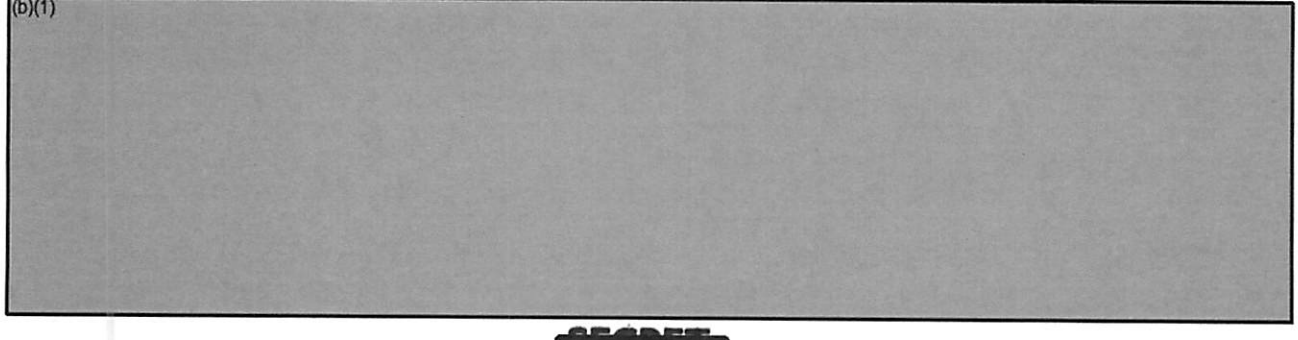
~~SECRET~~

(b)(1)



7. (U) Exercise Execution

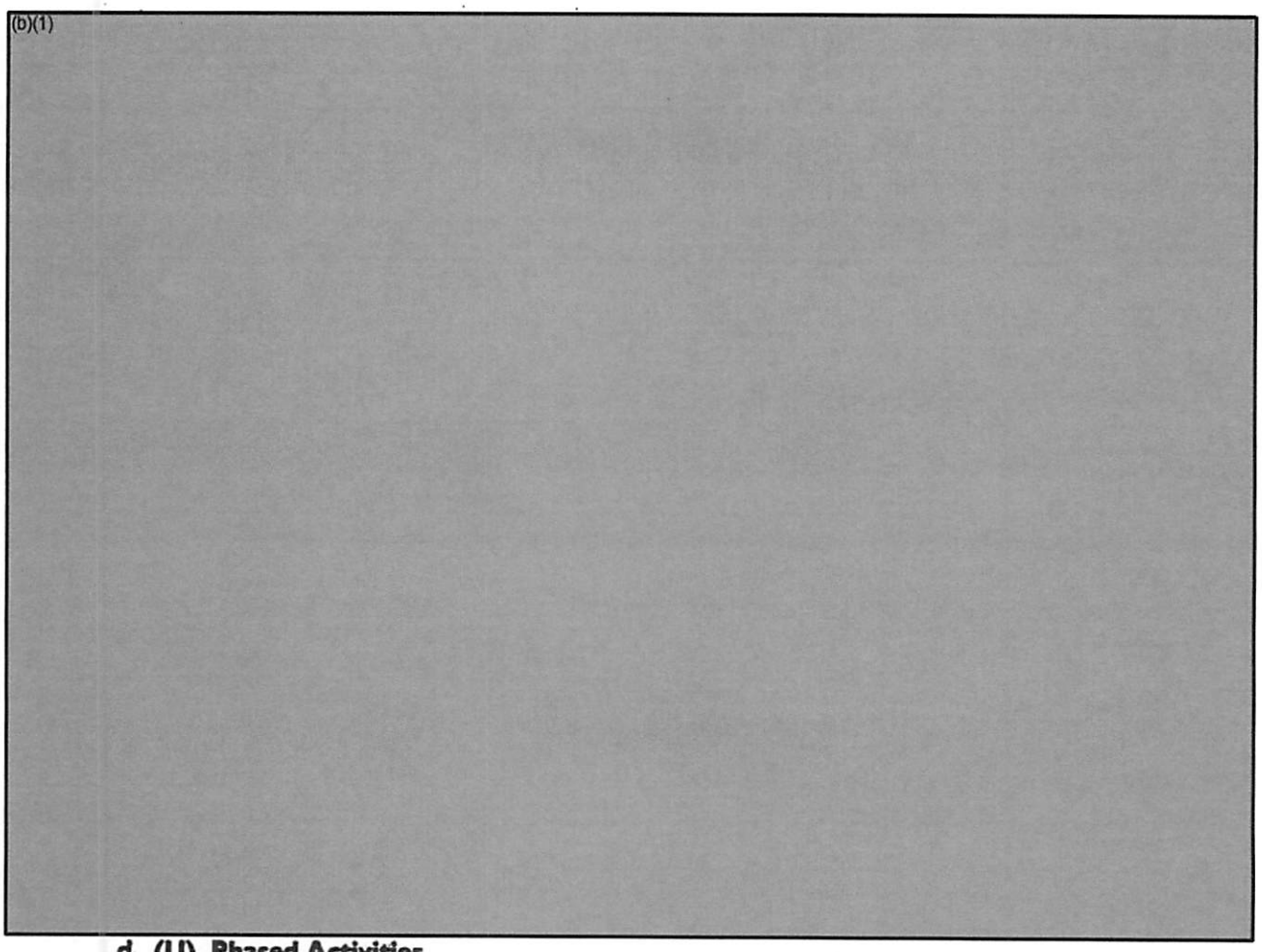
(b)(1)



~~SECRET~~

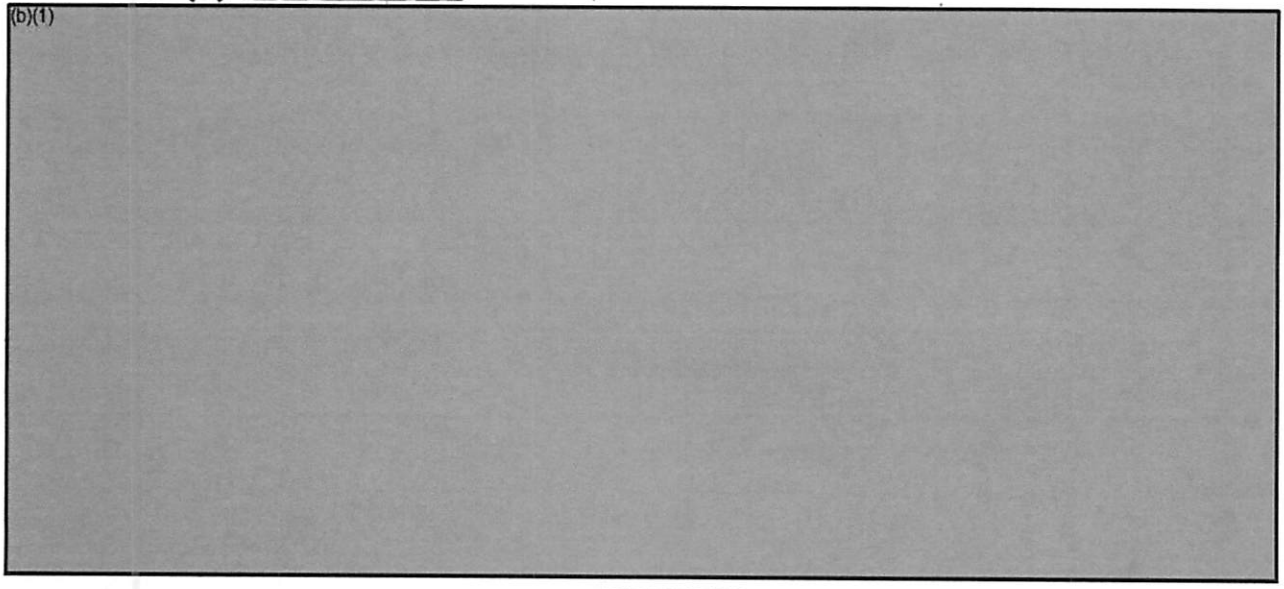
~~SECRET~~

(b)(1)



d. (U) Phased Activities

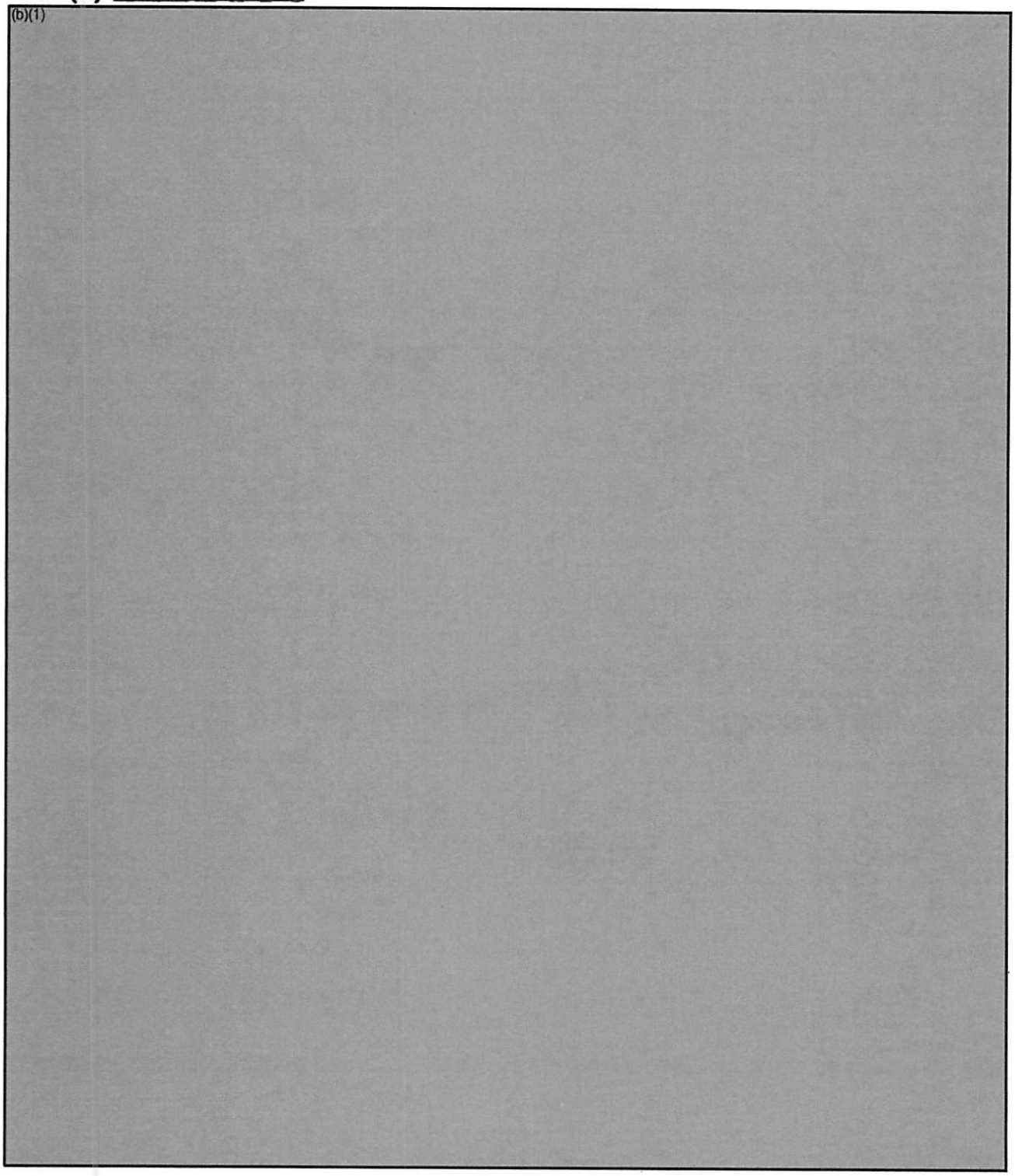
(b)(1)



~~SECRET~~

8. (U) The Active Threat

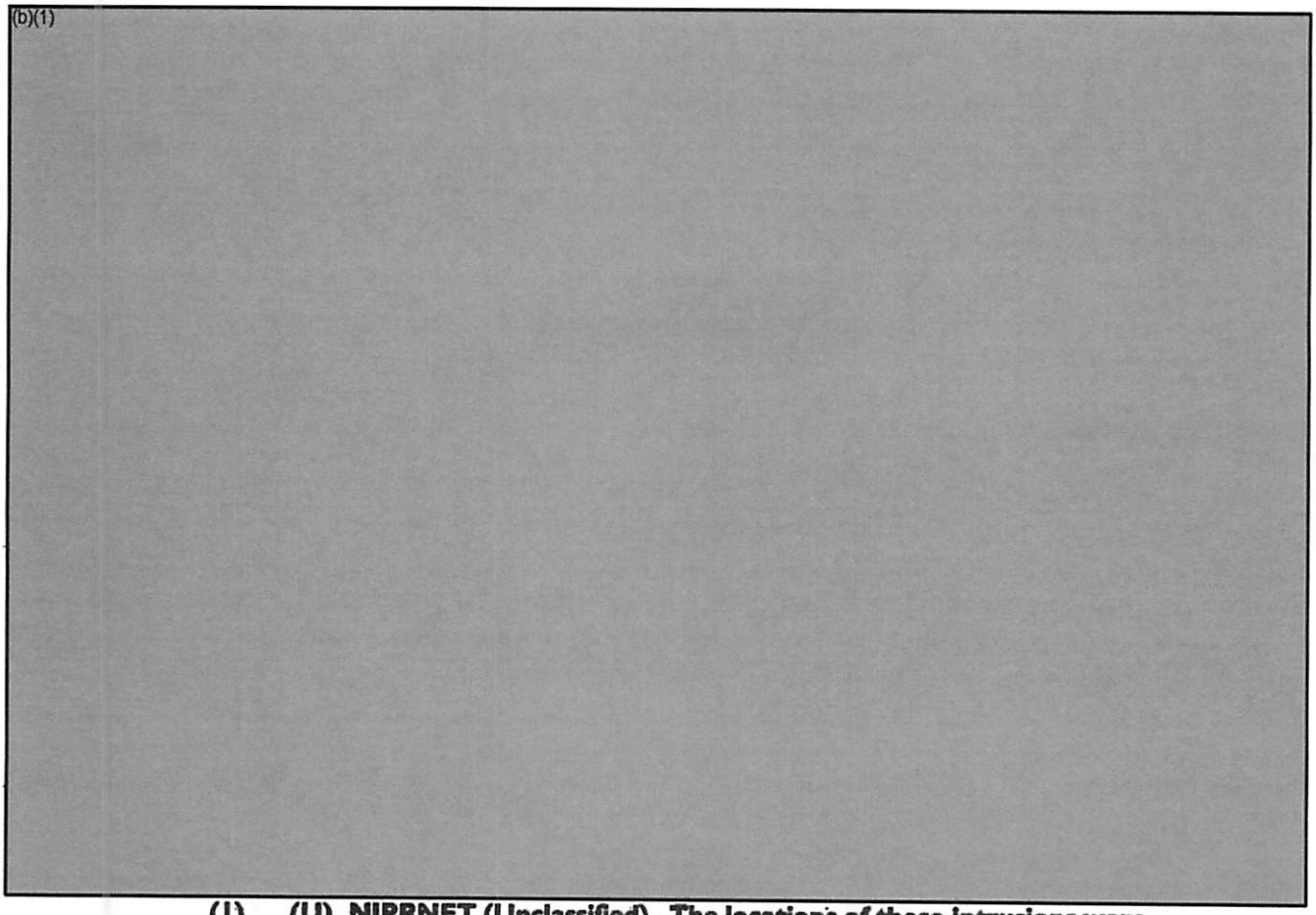
(b)(1)



~~SECRET~~

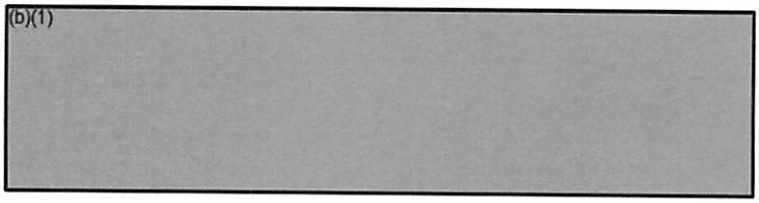
~~SECRET~~

(b)(1)



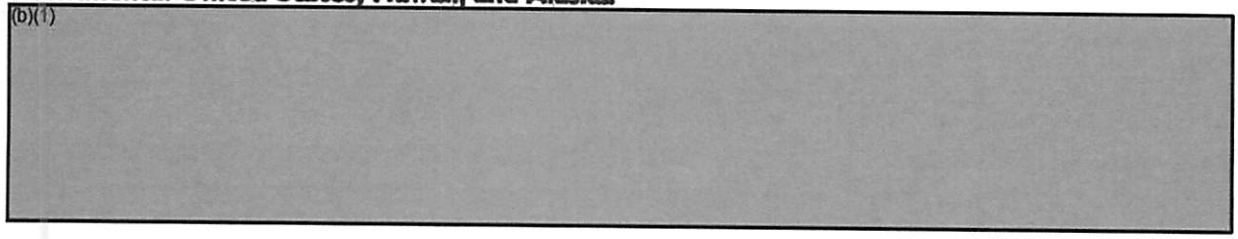
(1) (U) NIPRNET (Unclassified). The locations of these intrusions were worldwide.

(b)(1)

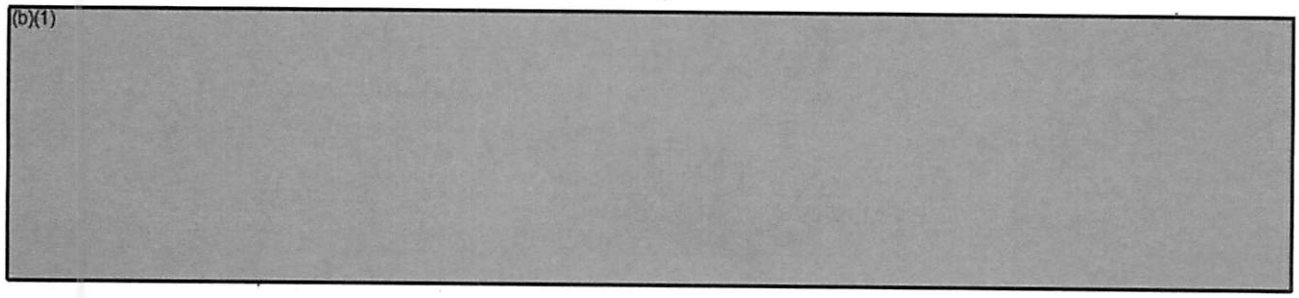


(2) (U) SIPRNET (Classified). The locations of these intrusions were limited to the continental United States, Hawaii, and Alaska.

(b)(1)



(b)(1)



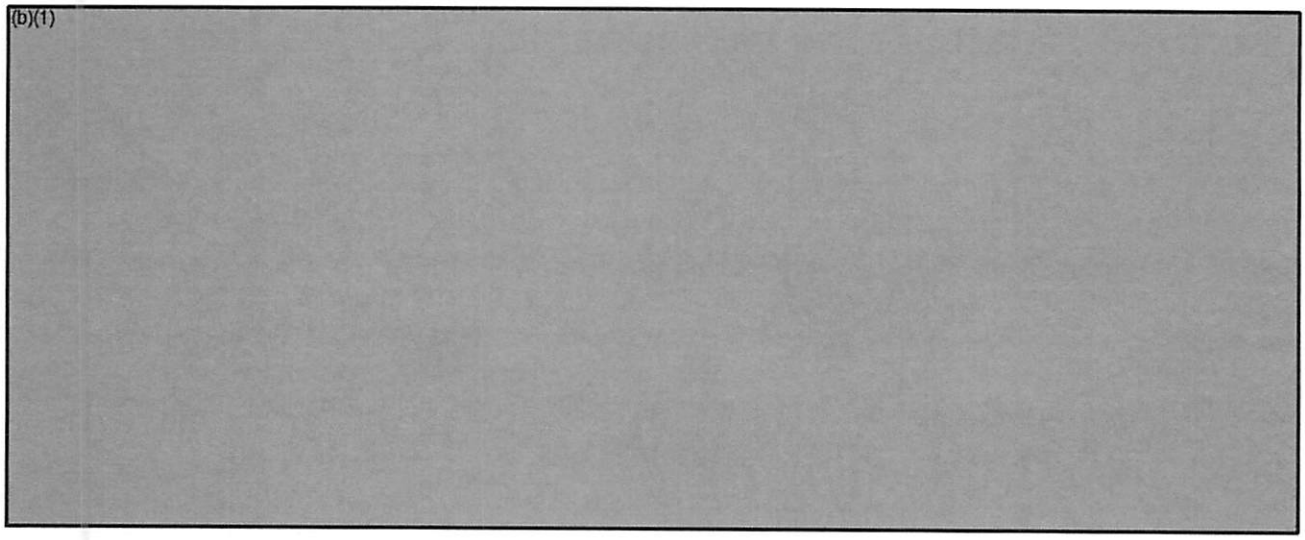
(INTENTIONALLY BLANK)

~~SECRET~~

CHAPTER II

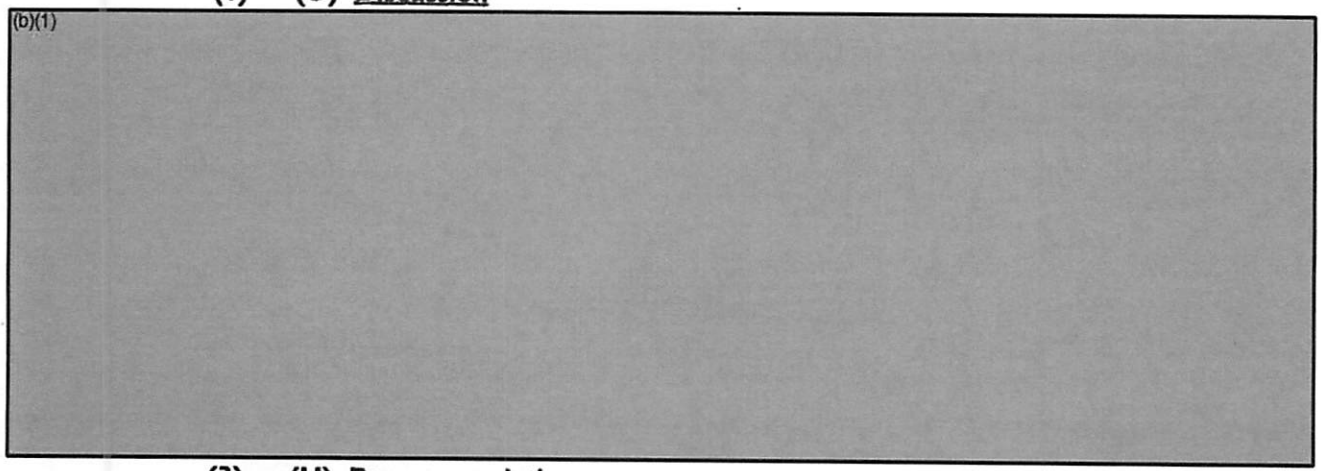
(U) AWARENESS AND UNDERSTANDING

(b)(1)



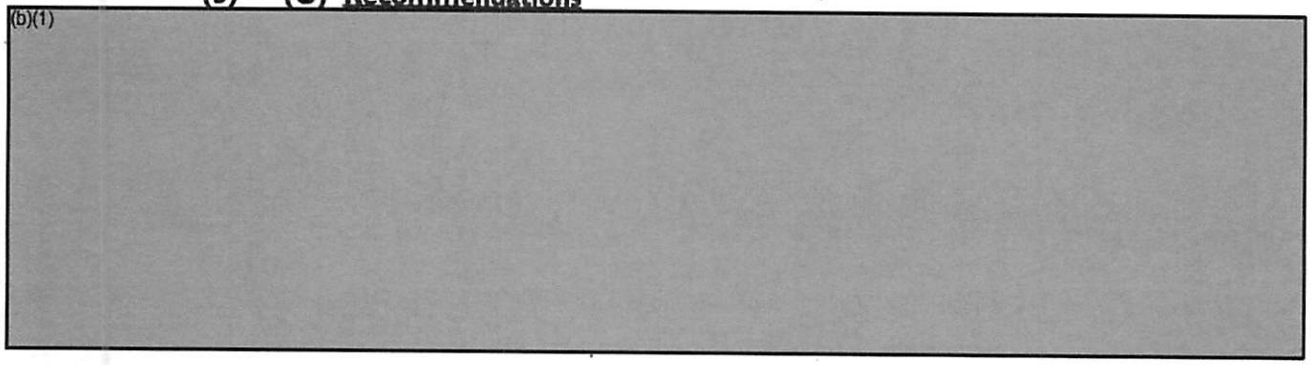
(1) (U) Discussion

(b)(1)



(3) (U) Recommendations

(b)(1)



(1) (U) Discussion

(a) (U) During the exercise several critical infrastructures were attacked, particularly power systems and DOD computer systems.

(b) (U) The DOD Critical Infrastructure Protection Working Group (CIPWG) is working the military aspects of infrastructure protection. The CIPWG is designed to consider issues, across components, that could be associated with the loss or disruption of specific national and defense infrastructures (telecommunications, electrical power systems, gas and oil storage and transport, water supply systems, banking and finance, transportation, emergency services, and continuity of government).

(c) (U) Infrastructure protection includes many government departments and agencies. It is not exclusively a DOD role.

(d) (U) USACOM, through Forces Command, has a role in the protection of national infrastructure assets.

(2) (U) Conclusion. Understanding various agency responsibilities and capabilities and how to coordinate unity of effort is required in dealing with attacks against the national infrastructure.

(3) (U) Recommendations

(a) (U) The DOD role in the protection of critical infrastructure, including the private sector, should be determined.

(b) (U) The role of industry in developing infrastructure protection responsibilities and procedures should be determined.

(c) (U) When to involve State, local, and private-sector officials, both during and after infrastructure attacks, should be determined.

(d) (U) A decision support structure to provide unity of effort in dealing with infrastructure attacks should be established.

(e) (U) The Department of Defense and other Government agencies should continue to conduct exercises in national infrastructure protection.

(f) (U) Since many of the above recommendations are already under active consideration by the Critical Infrastructure Protection Working Group (CIPWG), it may be appropriate that the CIPWG coordinate the overall effort.

(b)(1)

(1) (U) Discussion

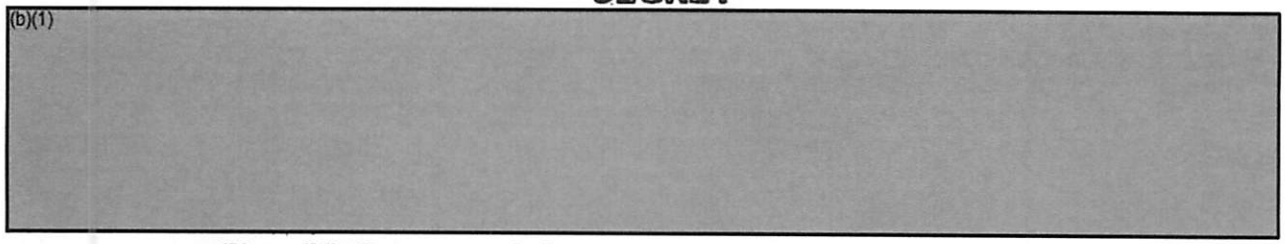
(a) (U) The exercise scenario included computer network attacks (CNAs) against DOD information systems. The reaction of the players to the CNAs demonstrated the need to train users and administrators on how to protect their systems from attack and measures that should be taken in response to intrusions or attacks.

(b) (U) The Red Team was able to take advantage of system security vulnerabilities that should have been closed by either properly trained users or system administrators. Some examples include the use of simple passwords, improper configuration of system networks, and operations security (OPSEC) of particular system Internet protocol (IP) names.

(c) (U) The Red Team found large amounts of unclassified computer home pages that would assist a potential attacker.

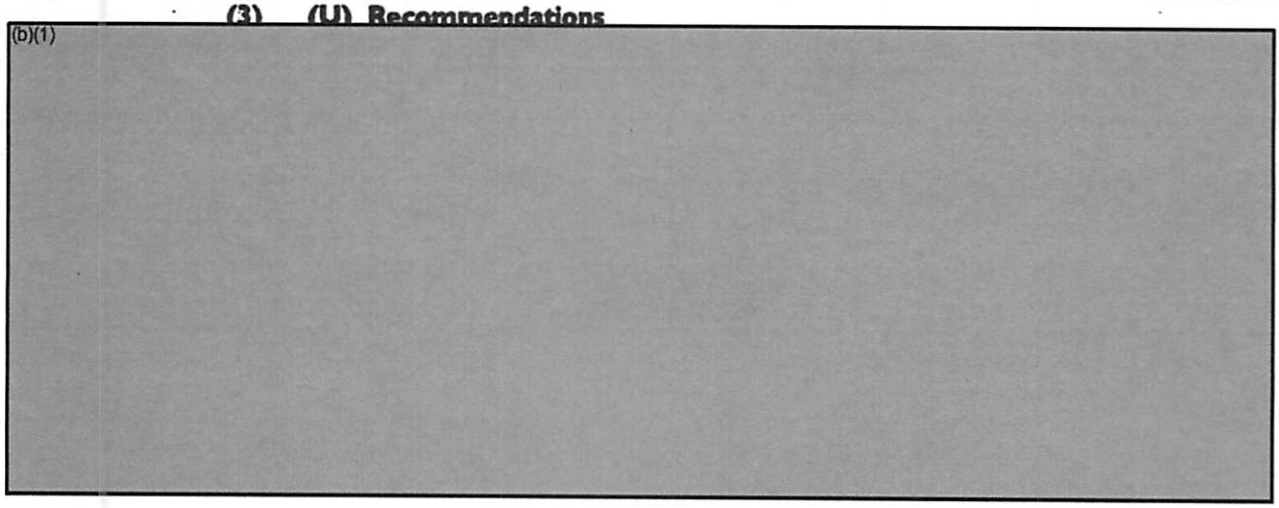
~~SECRET~~

(b)(1)



(3) (U) Recommendations

(b)(1)



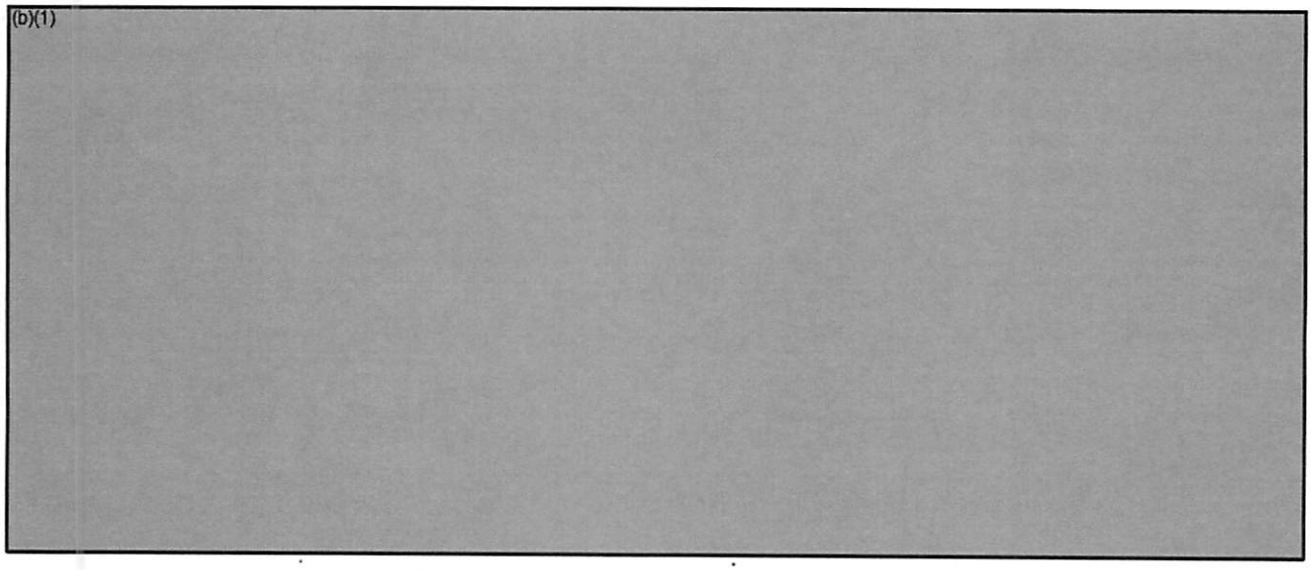
(INTENTIONALLY BLANK)

~~SECRET~~

CHAPTER III

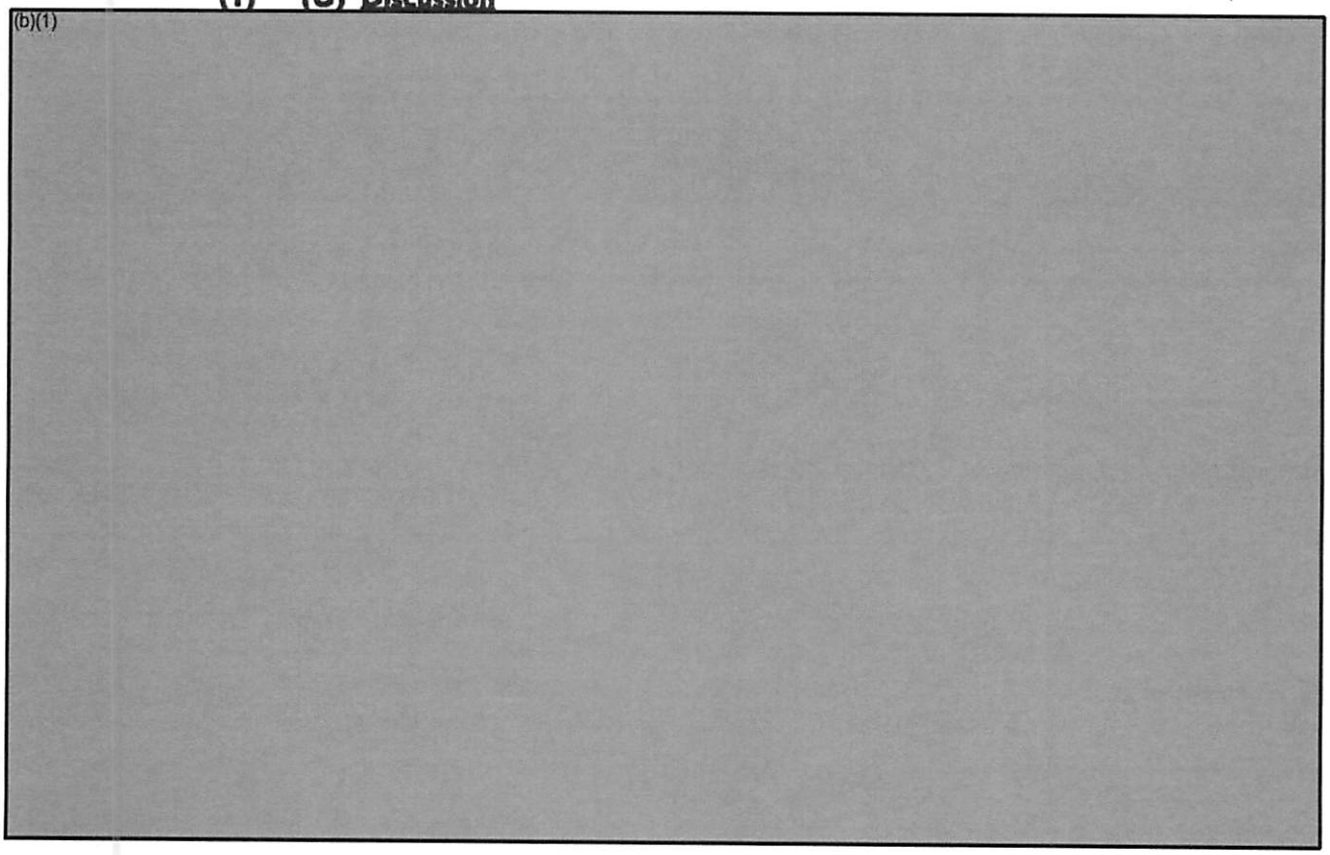
(U) POLICY ISSUES

(b)(1)



(U) Discussion

(b)(1)



(b)(1)

(3) (U) Recommendations

(b)(1)

b. (U) Observation. There were no policies or procedures that established clear responsibility for directive authority or control over numerous nodes of the Defense Information Infrastructure (DII). In ER97-1, there was nearly a situation with a commander in chief (CINC) saying block it and the Global Operations and Security Center (GOSC) saying leave it open for a router suspected of being penetrated.

(1) (U) Discussion

(b)(1)

(1) (U) Discussion

(b)(1)

~~SECRET~~

(b)(1)

[redacted]

(3) (U) Recommendations

(b)(1)

[redacted]

(3) (U) Recommendations

(b)(1)

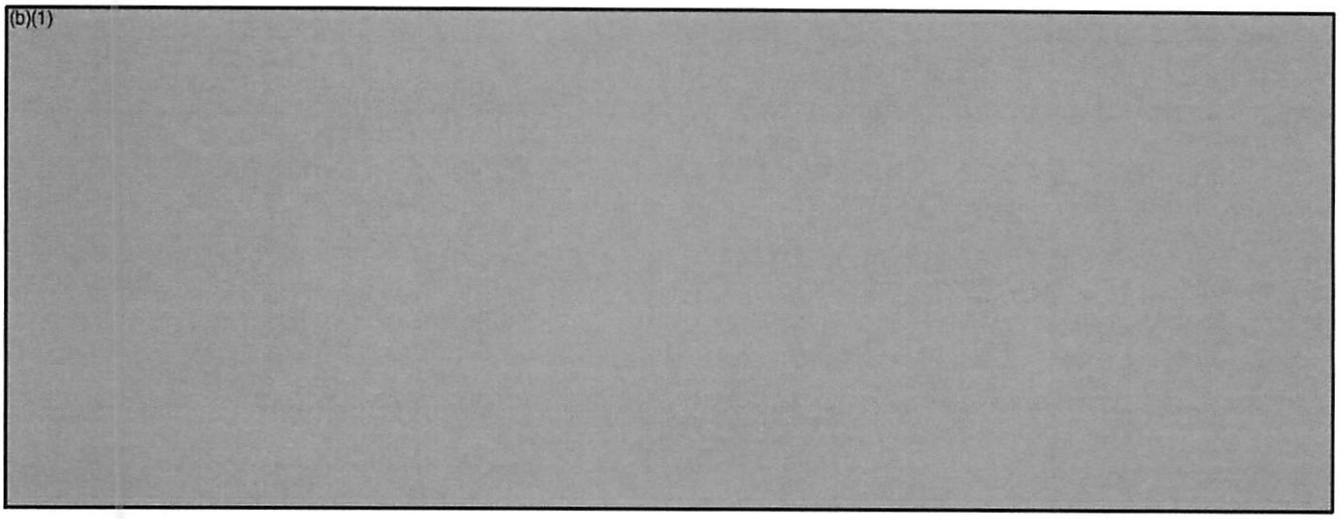
[redacted]

~~SECRET~~

CHAPTER IV

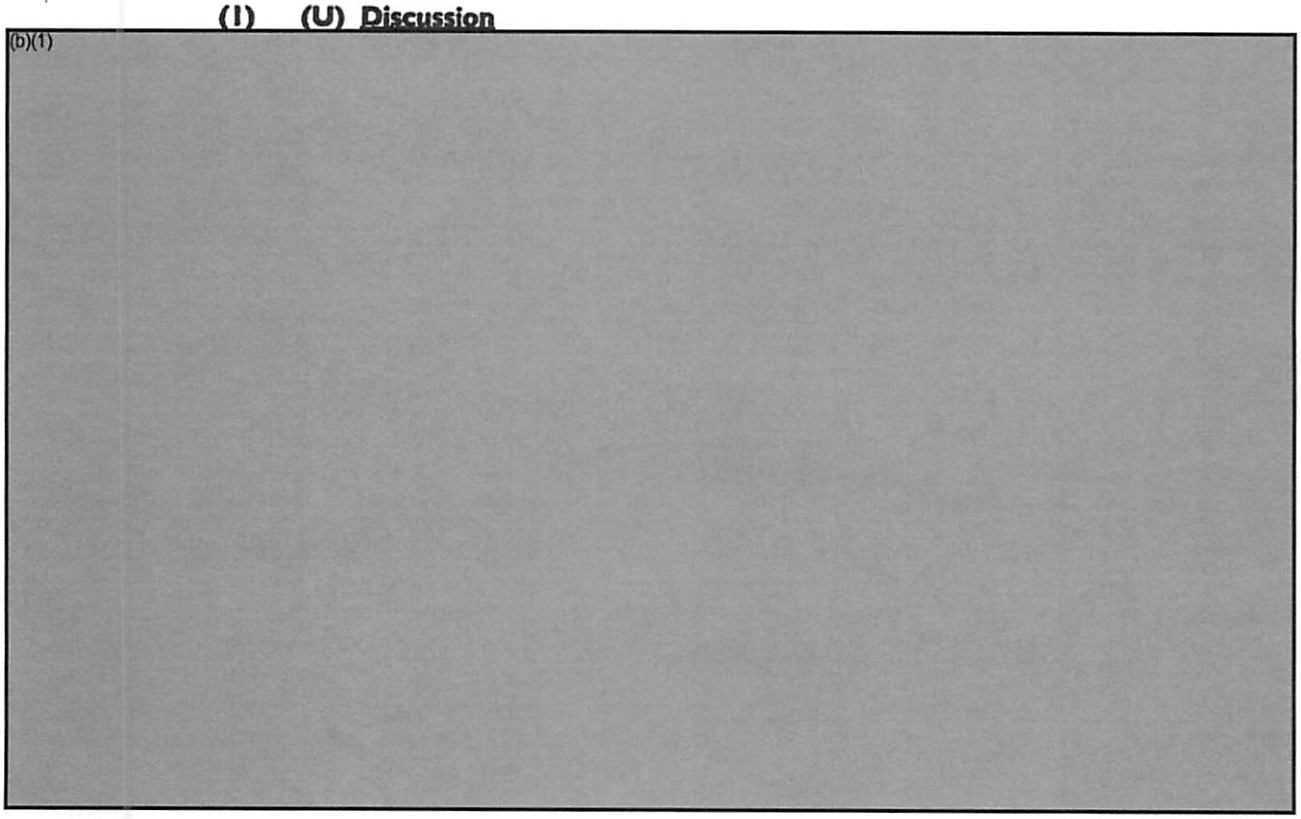
(U) INTERAGENCY COORDINATION ISSUES

(b)(1)



(I) (U) Discussion

(b)(1)



~~SECRET~~

(b)(1)

[redacted]

(1) (U) Discussion

(a) (U) Jurisdiction for defending against information operations depends on the identity and location of the perpetrators.

(b)(1)

[redacted]

(2) (U) Conclusions

(b)(1)

[redacted]

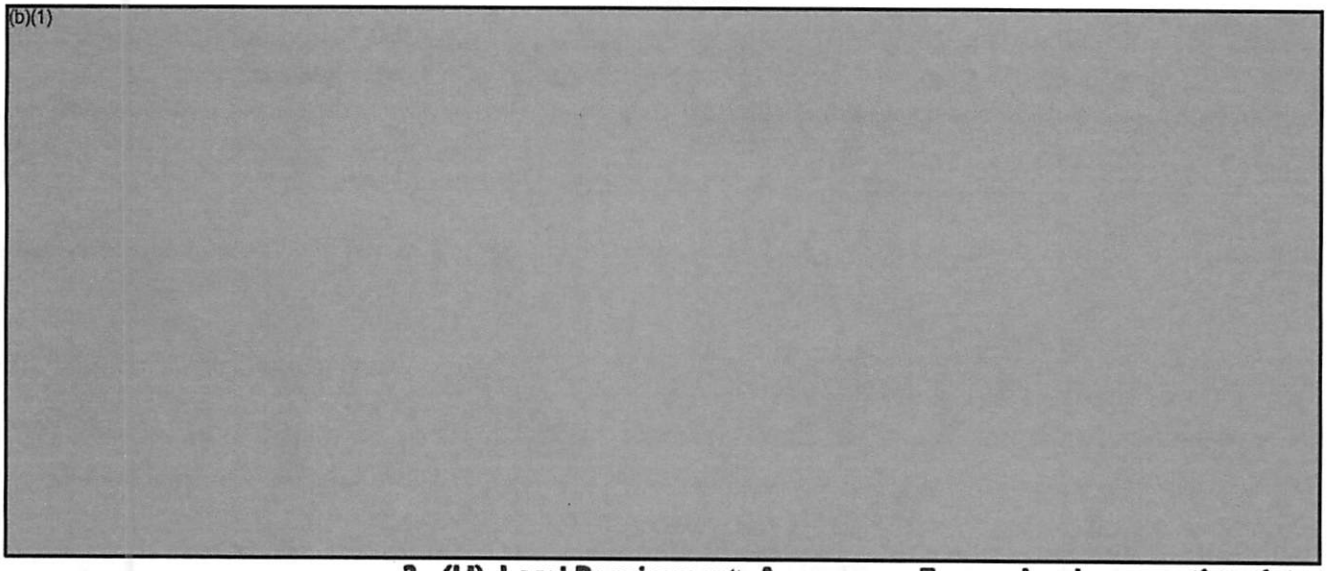
(1) (U) Discussion

(b)(1)

[redacted]

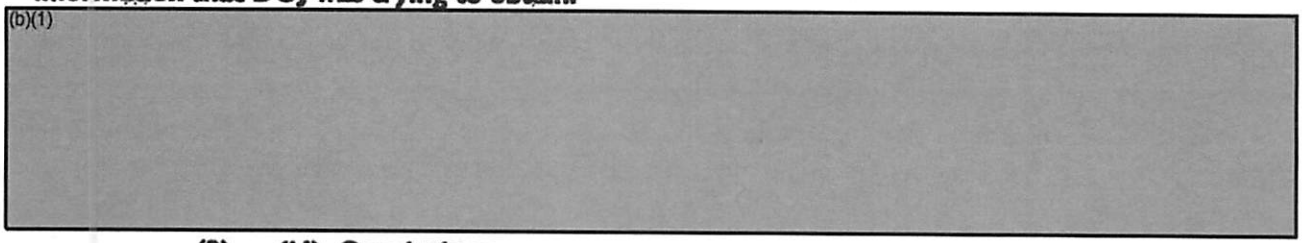
~~SECRET~~

(b)(1)



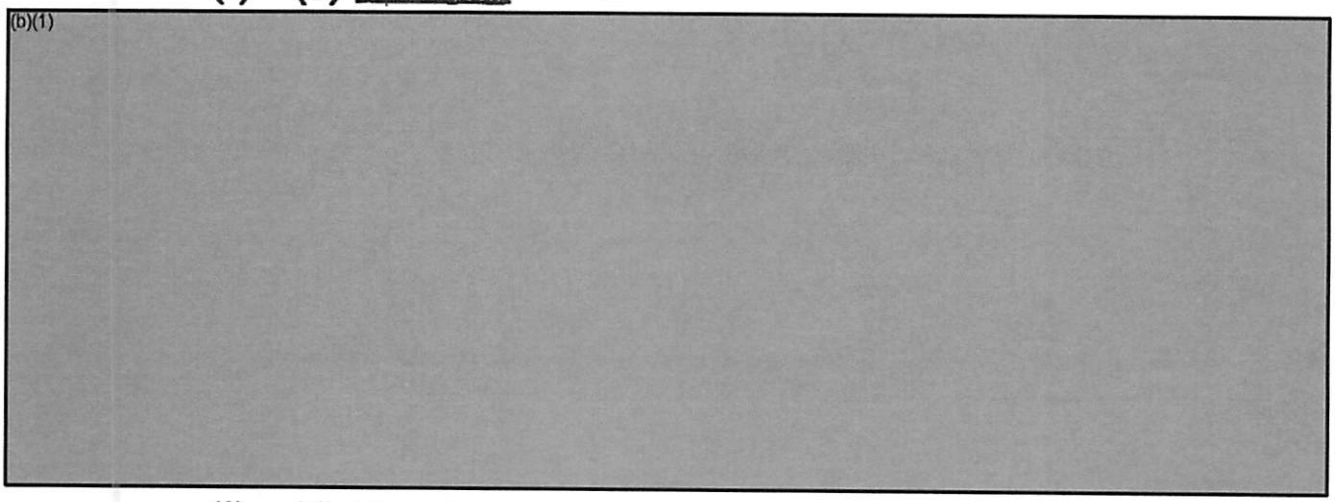
2. (U) Legal Requirements Awareness. From a legal perspective, the Department of Justice (DOJ) was proactive in obtaining court orders in Guam to allow for communication intercepts from the ship. Unbeknownst to DOJ, the military was already intercepting International Maritime Satellite (INMARSAT) communications and had the information that DOJ was trying to obtain.

(b)(1)



(2) (U) Conclusions

(b)(1)



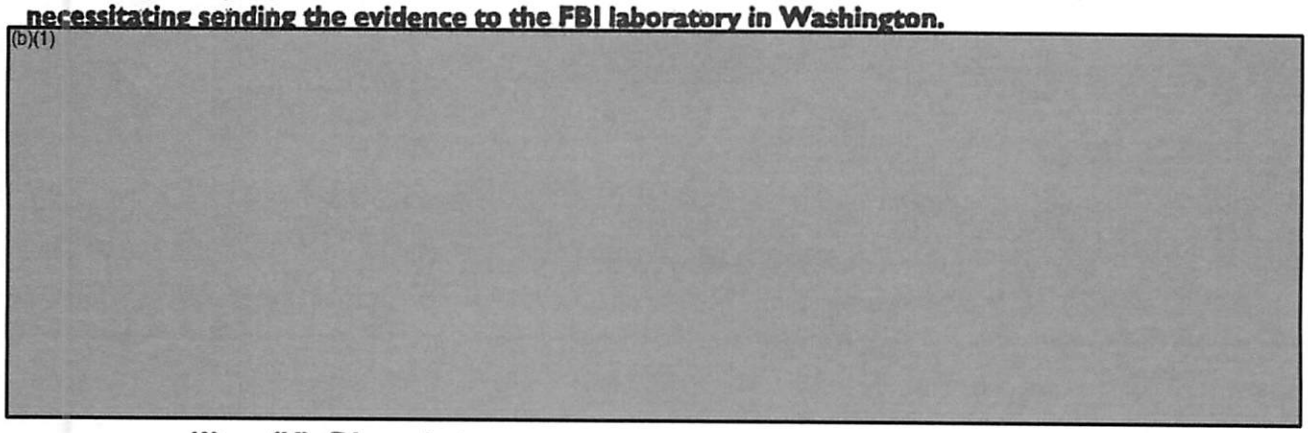
(I) (U) Discussion

(a) (U) The Department of Defense and DOJ had conflicting goals regarding captured individuals and equipment. The DOD idea was a quick preliminary intelligence

assessment of any captured material. DOJ and the DEST configuration were oriented toward evidence and prosecution, not on-scene IO intelligence.

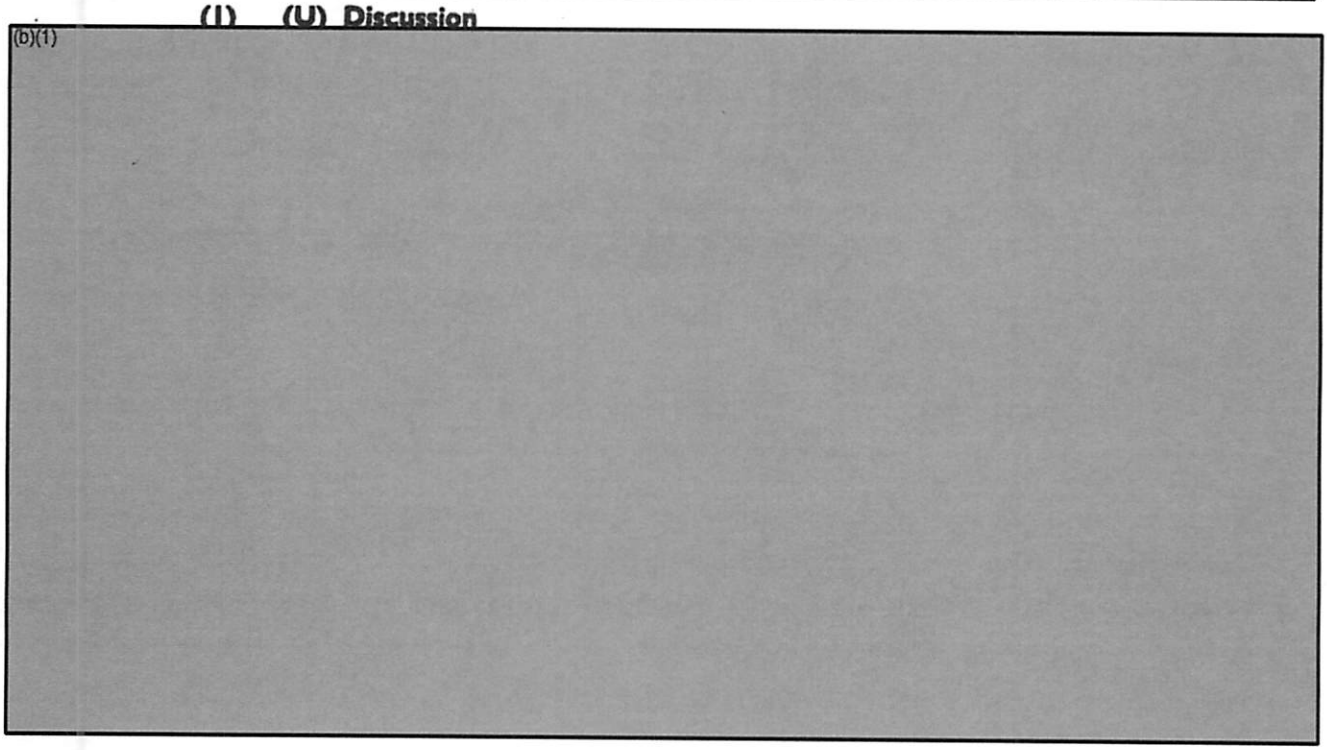
(b) (U) The notional modification to the DEST was insufficient to permit on-site review of the disk. The disk had to be notionally transported to Washington, DC for analysis and evidence (needs of the FBI) but did not satisfy the DOD need for on-sight analysis for intelligence purposes. Local technical resources in Guam were also insufficient, thus necessitating sending the evidence to the FBI laboratory in Washington.

(b)(1)



(1) (U) Discussion

(b)(1)



f. (U) Observation. The Joint Staff understood it needed the DISA Liaison Team but did not know how to use it.

(1) (U) Discussion

(a) (U) The Joint Staff knew that either coordination with or information

from DISA was critical for the exercise scenario that was presented to them.

(b) (U) The DISA Liaison Team was requested and was used as an extension of the Joint Staff to get questions answered.

(c) (U) The team had no work area the first day. The following days, the only automation support was a personal computer with word processing.

(d) (U) Electronic interchange of information between the team and DISA headquarters was nonexistent. Only a secure telephone unit (STU) and a facsimile machine were available.

(e) (U) Multiple people from the Joint Staff J-2, J-3, and J-6 tasked the DISA Liaison Team with variants of the same questions. There was no coordination of taskings from the Joint Staff.

(f) (U) There was no prioritization of tasks related to their importance.

(2) (U) Conclusion. Joint Staff use of the DISA Liaison Team was inefficient.

(3) (U) Recommendations

(a) (U) DISA and the Joint Staff should coordinate the role and duties of liaison teams and arrange adequate workspace, secure communications, and procedures to exchange information.

(b) (U) The Joint Staff should establish procedures to ensure liaison teams are not tasked several times for the same information.

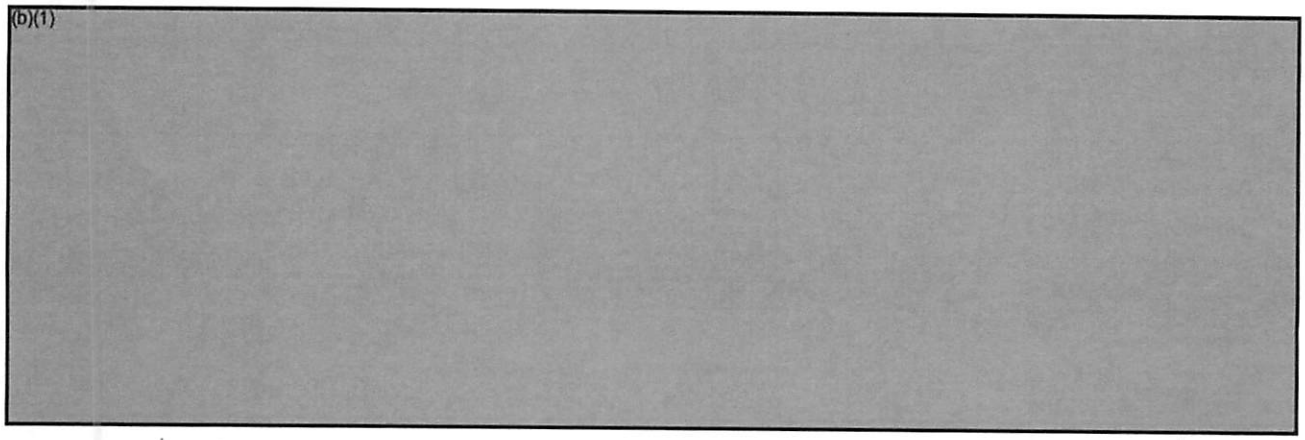
(INTENTIONALLY BLANK)

~~SECRET~~

CHAPTER V

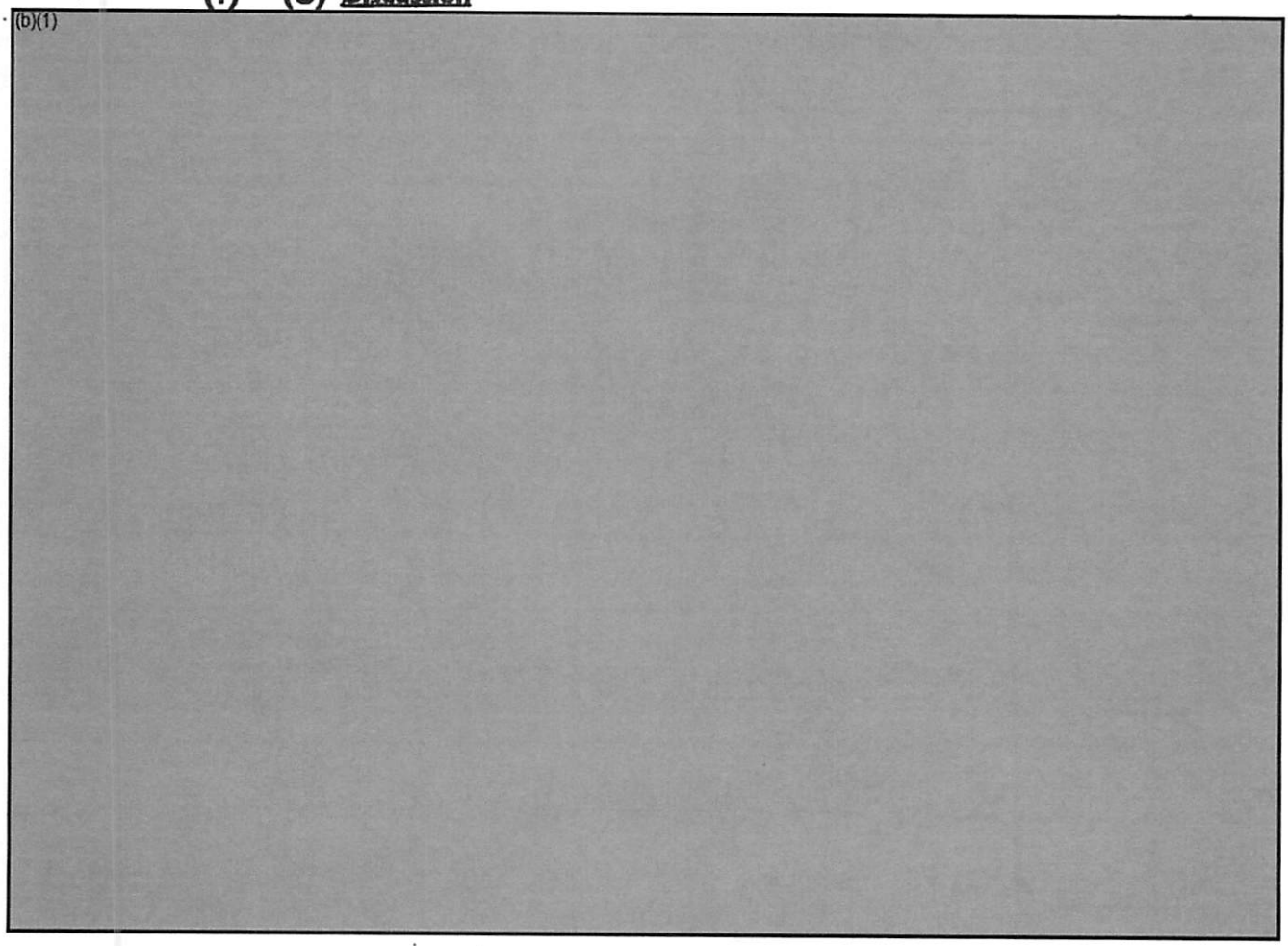
(U) PLANNING, PROCEDURES, AND PROCESSES ISSUES

(b)(1)



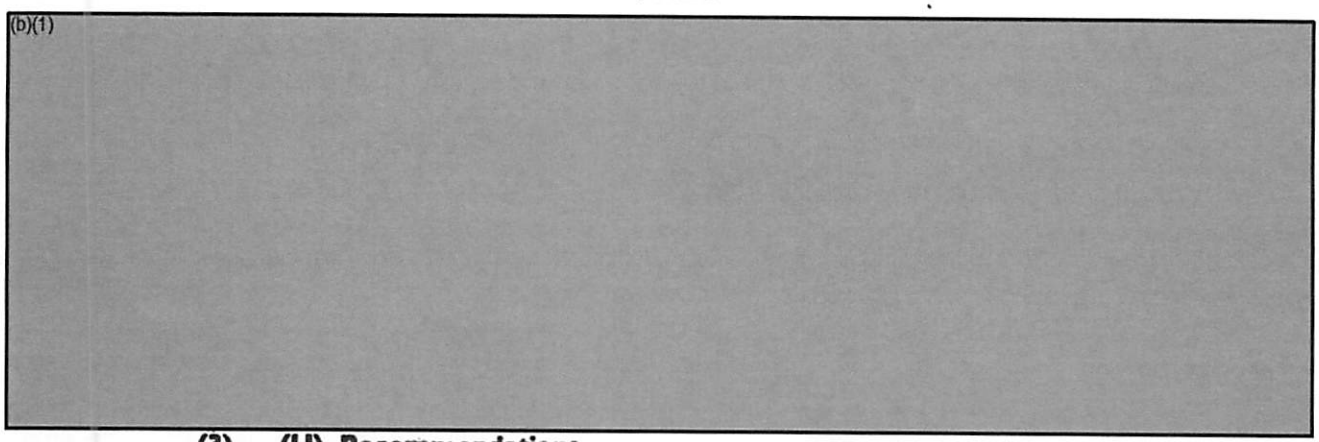
(I) (U) Discussion

(b)(1)



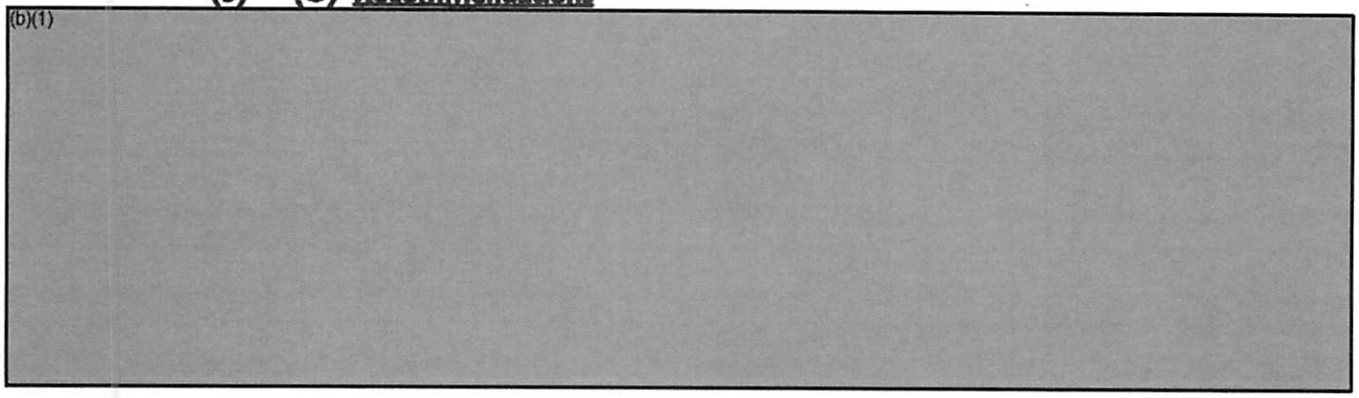
~~SECRET~~

(b)(1)



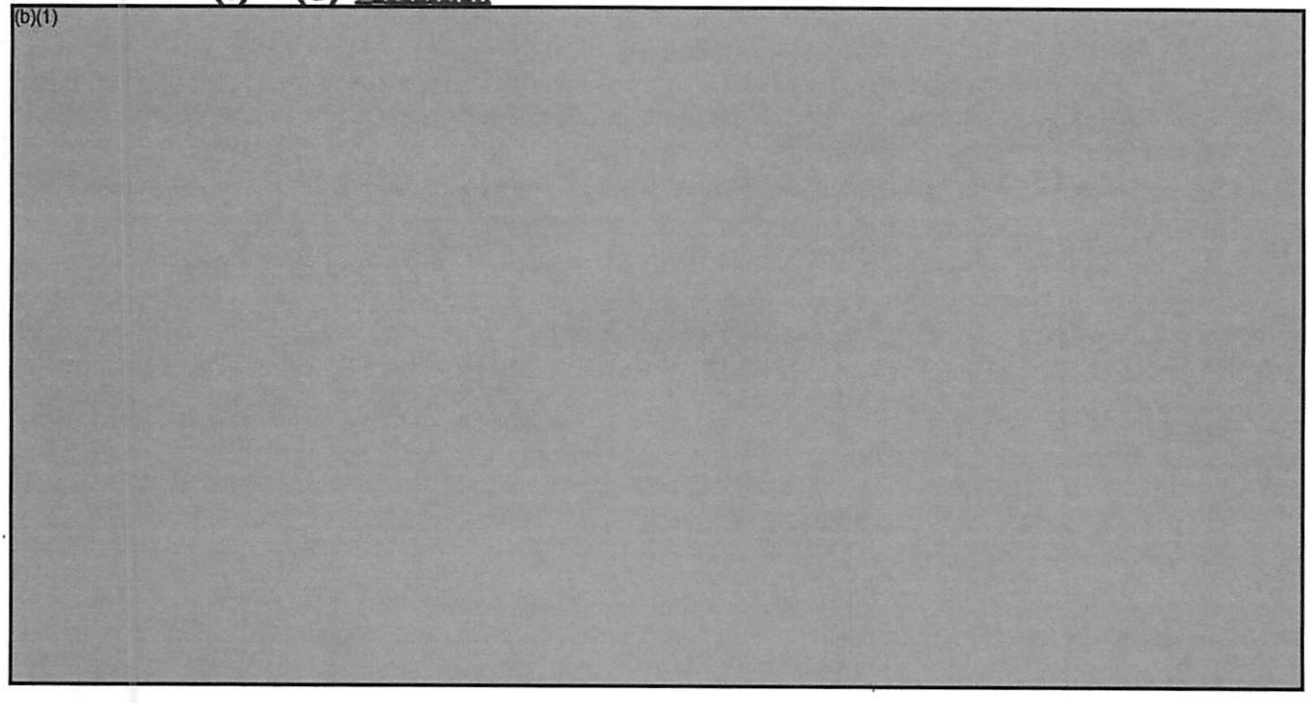
(3) (U) Recommendations

(b)(1)



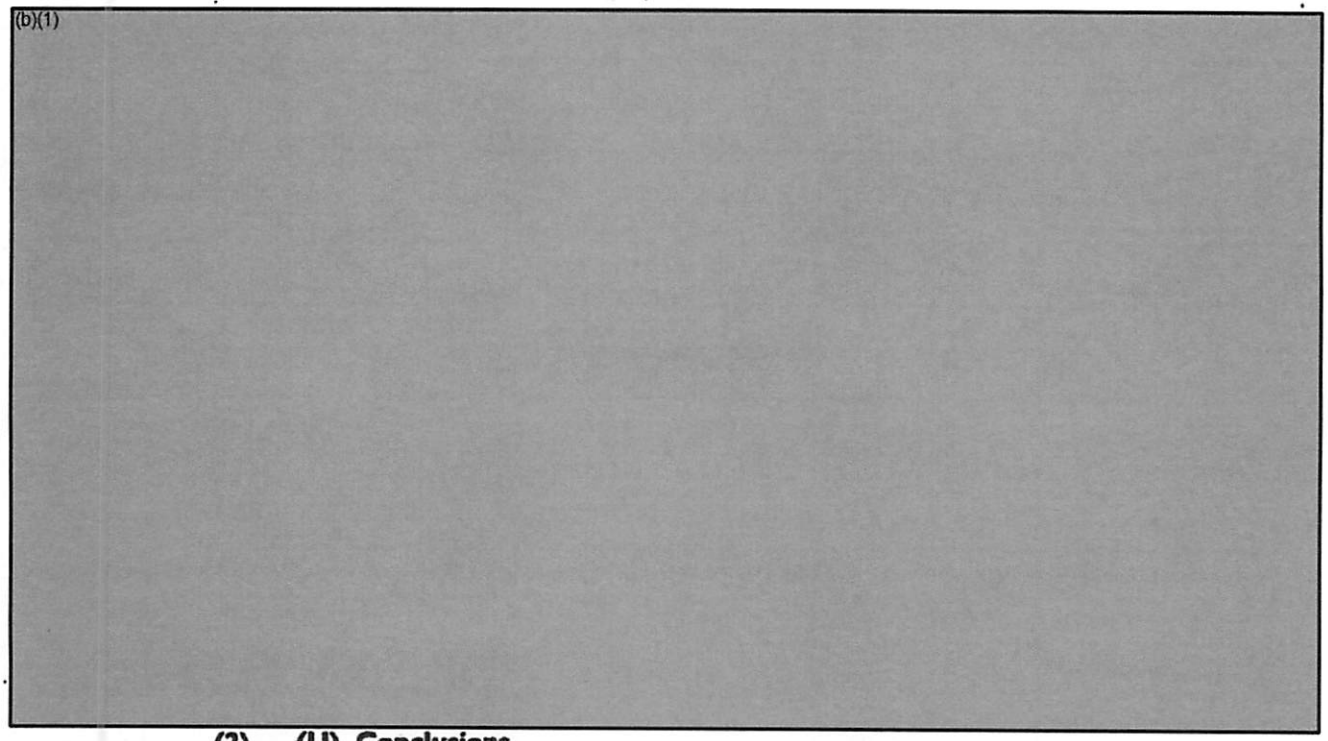
(I) (U) Discussion

(b)(1)



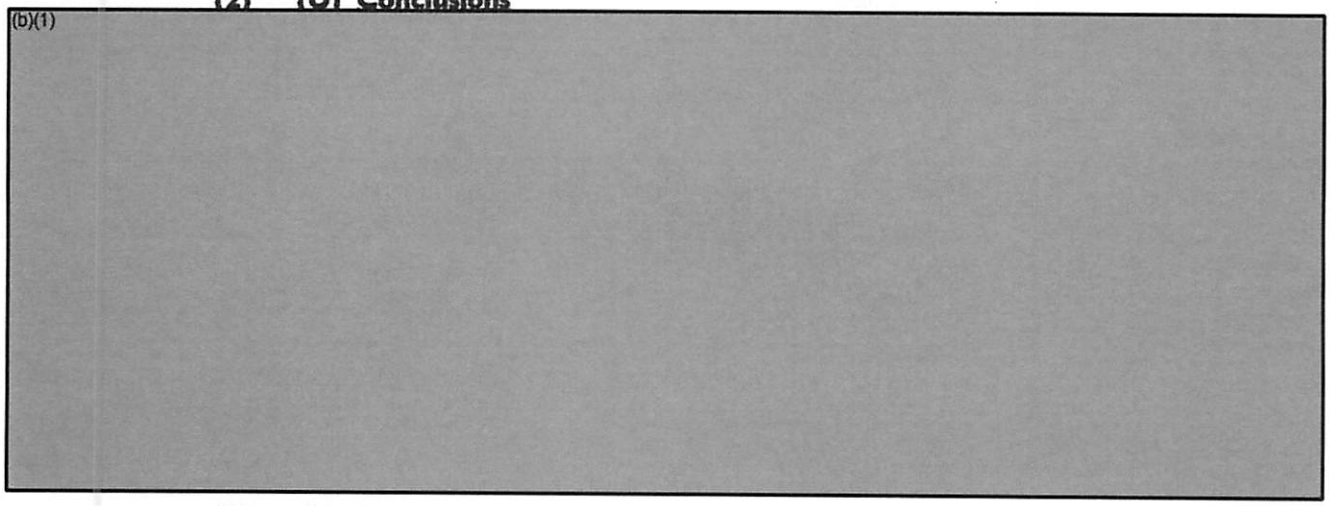
~~SECRET~~

(b)(1)



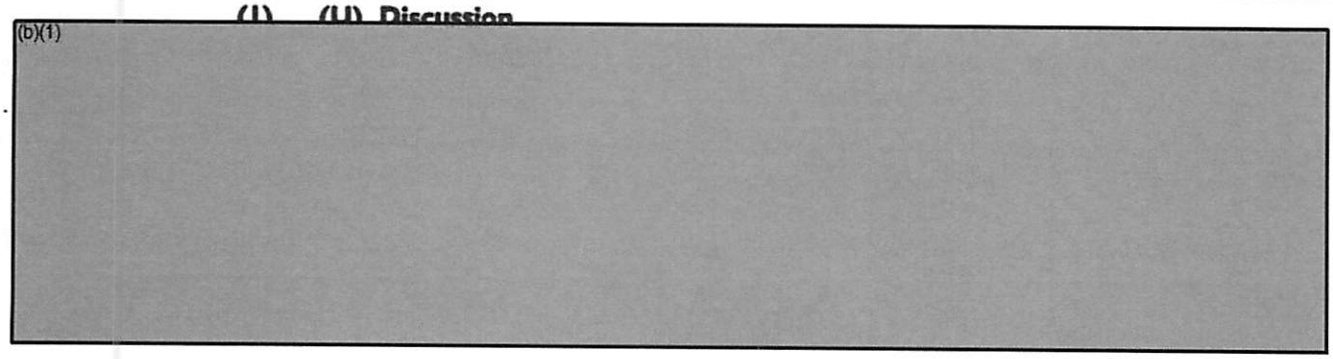
(2) (U) Conclusions

(b)(1)



(1) (U) Discussion

(b)(1)



~~SECRET~~

mechanism were missing.

(c) (U) Questions for which answers were not clear included the following:

(b)(1)

2. (U) Who pays?

(b)(1)

(2) (U) Conclusion. There is no policy or system for issuing alerts to industry or the public for infrastructure protection.

(b)(1)

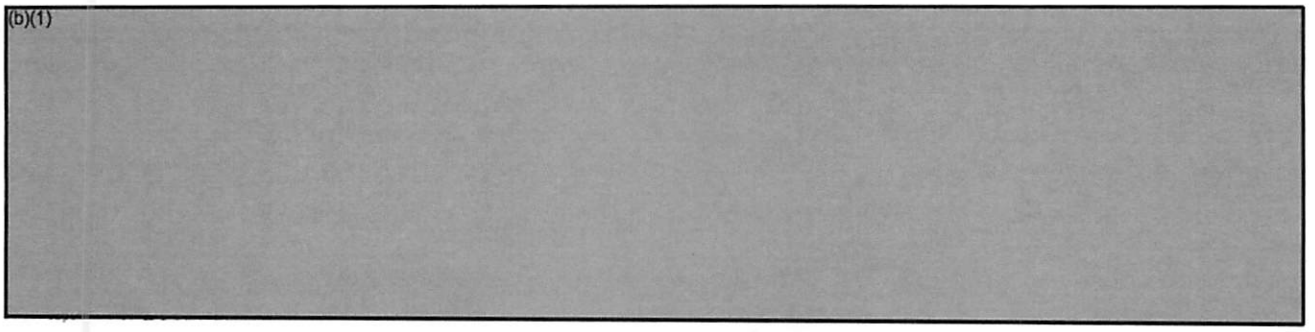
(1) (U) Discussion

(b)(1)

(d) (U) While the number of potentially vulnerable systems and accounts appear to be significantly large, a truly dedicated adversary would have taken much more time (i.e., months or years) to develop an extensive list of candidate accounts for exploitation and would have been willing to sacrifice some of his reconnaissance capabilities just to attain his goal. The number of detections may also be skewed a bit on the low side because some detections were not formally reported due to their association with the exercise.

(b)(1)

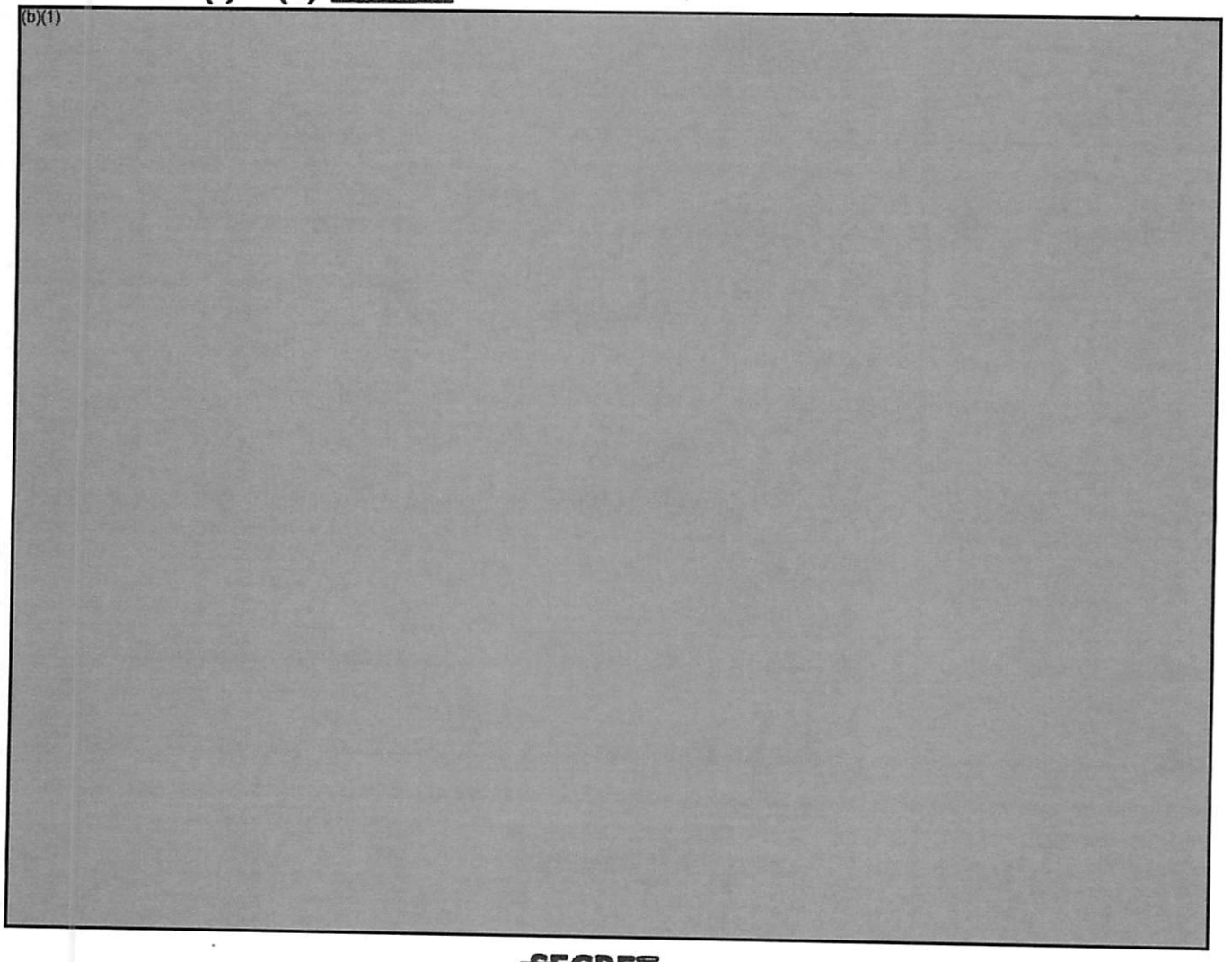
(b)(1)



e. (U) Observation. Even when they became aware that attacks on information systems were being widely reported, few organizations took additional defensive measures to preclude impact on their systems.

(1) (U) Discussion

(b)(1)



~~SECRET~~

(b)(1)

[redacted]

(I) (U) Discussion

(b)(1)

[redacted]

(I) (U) Discussion

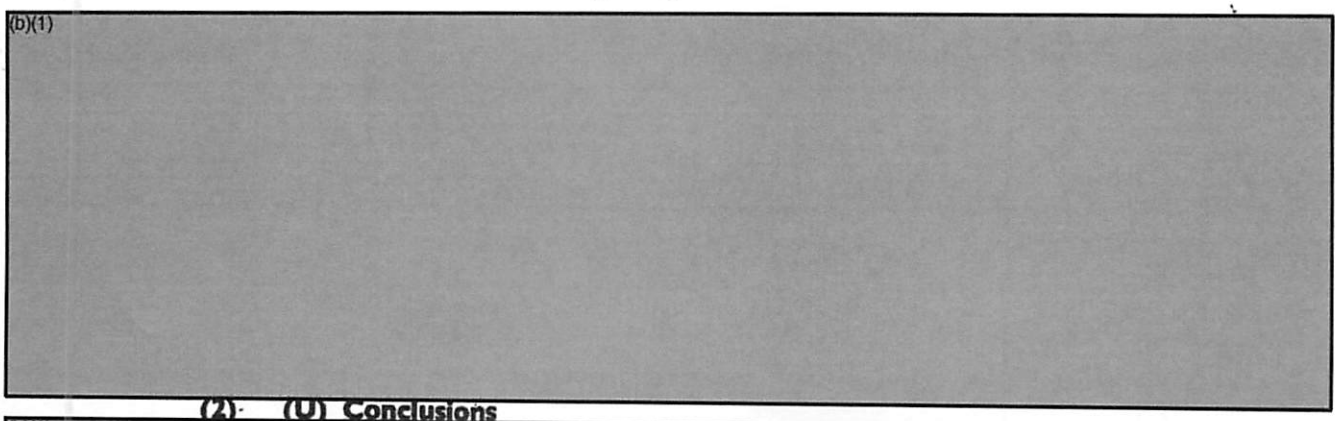
(b)(1)

[redacted]

~~SECRET~~

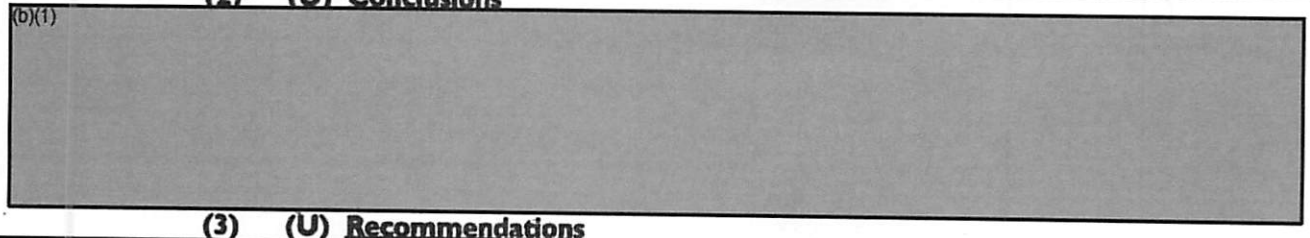
~~SECRET~~

(b)(1)



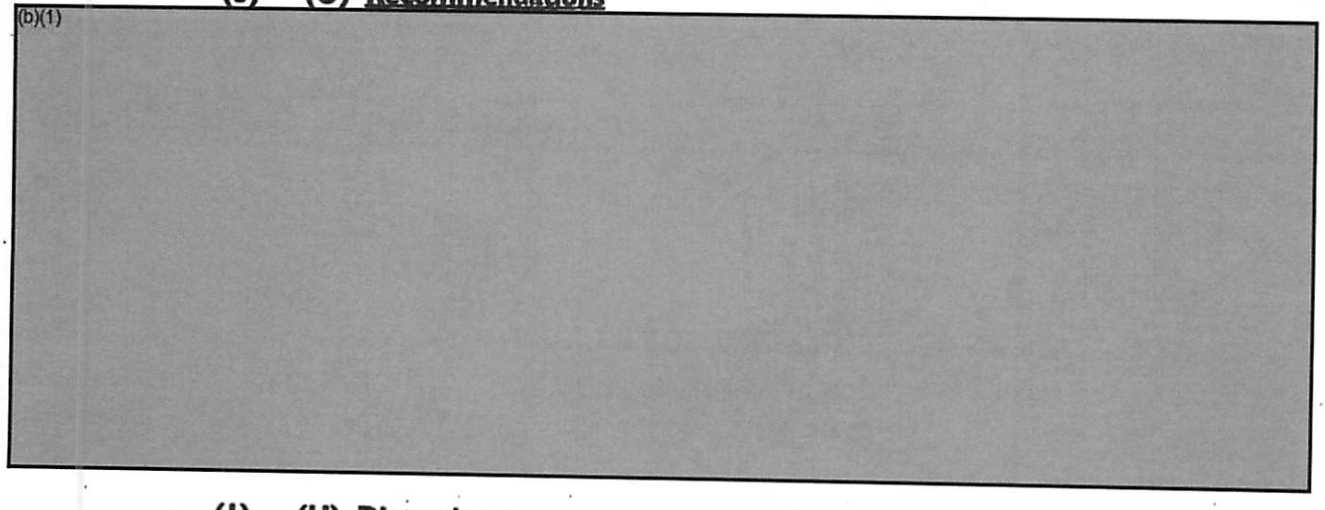
(2) (U) Conclusions

(b)(1)



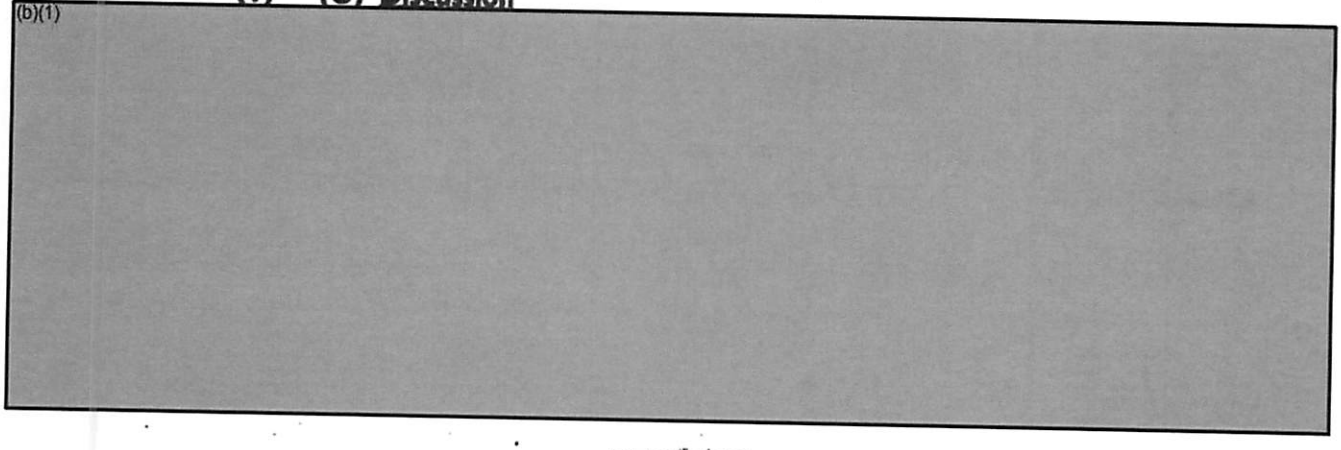
(3) (U) Recommendations

(b)(1)



(U) Discussion

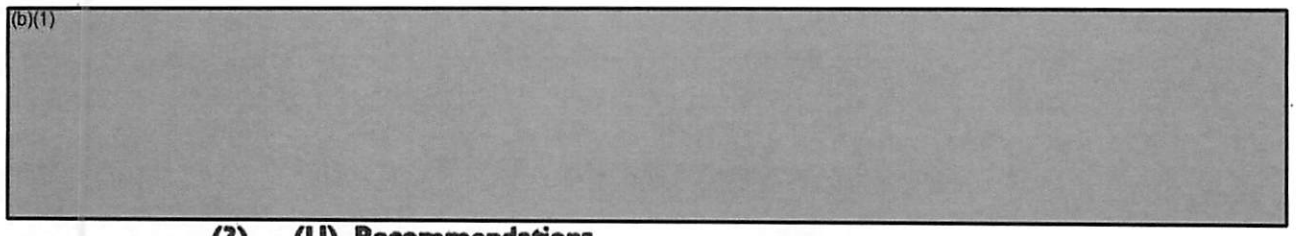
(b)(1)



~~SECRET~~

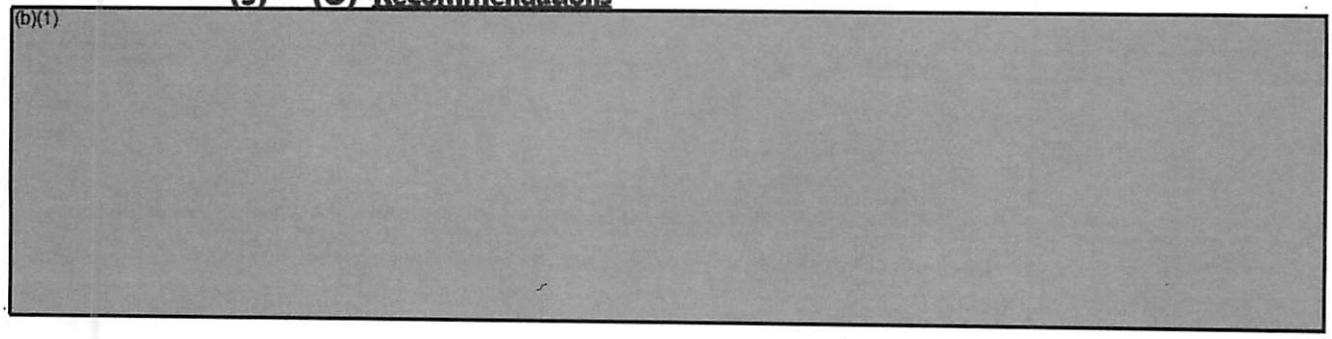
~~SECRET~~

(b)(1)



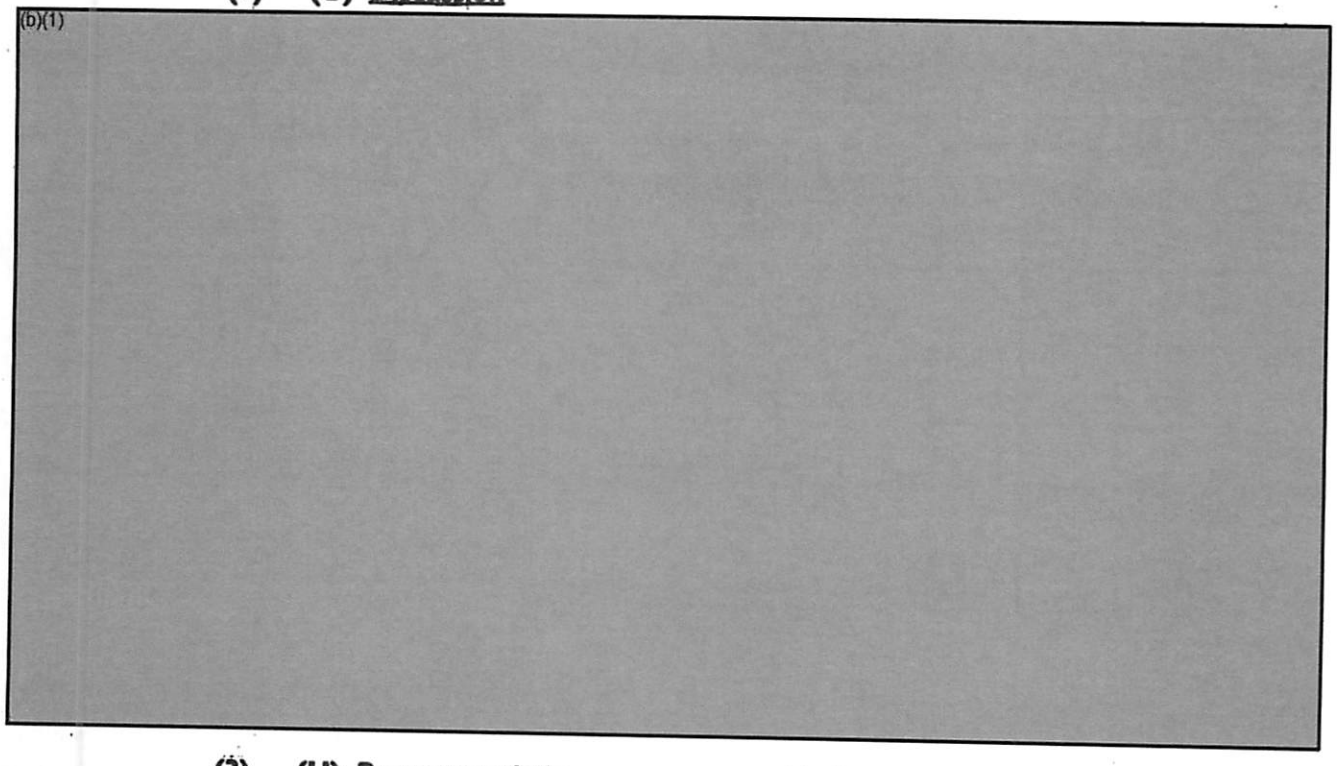
(3) (U) Recommendations

(b)(1)



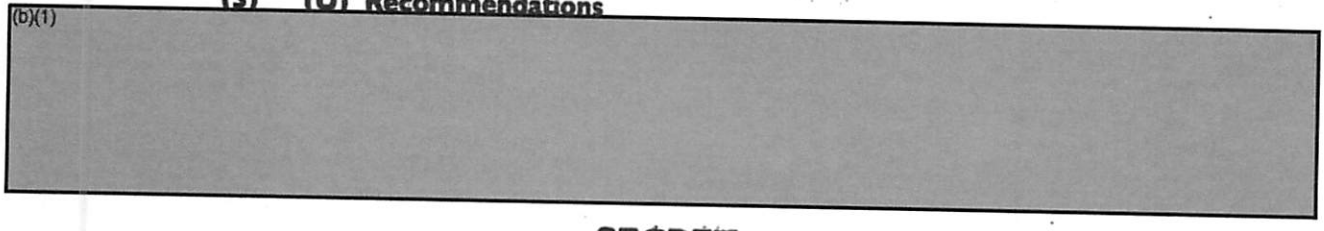
(I) (U) Discussion

(b)(1)



(3) (U) Recommendations

(b)(1)



~~SECRET~~

~~SECRET~~

(b)(1)

(1) (U) Discussion

(a) (U) Not all CERTs are manned for 24-hour operations and were not manned 24 hours during the exercise.

(b) (U) CERTs may not have contingency plans to support 24-hour operations.

(b)(1)

(3) (U) Recommendations

(b)(1)

k. (S) Observation. There was no evidence of coordination of defensive Information Operations to parallel Defense Readiness Conditions (DEFCONS) or Threat Conditions (THREATCONS).

(1) (U) Discussion

(b)(1)

(2) (U) Conclusion. No approved IO THREATCONs exist.

(3) (U) Recommendations

(b)(1)

~~SECRET~~

(b)(1)

(I) (U) Discussion

(b)(1)

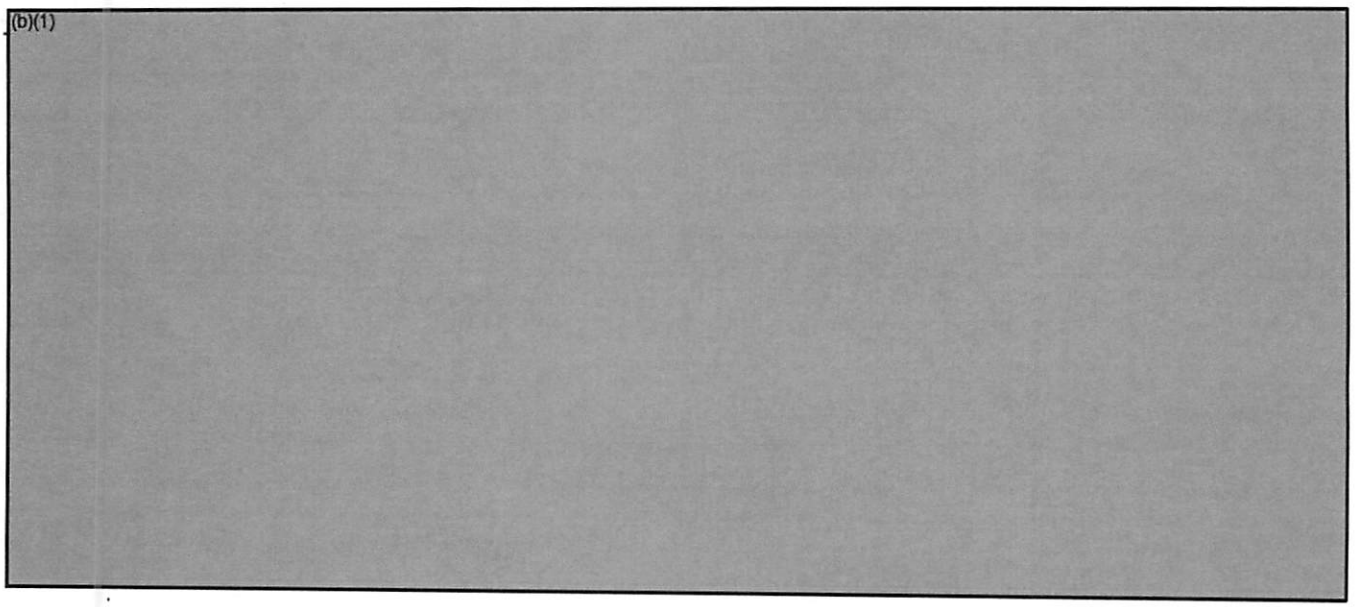
(3) (U) Recommendations

(b)(1)

(I) (U) Discussion

(b)(1)

(b)(1)

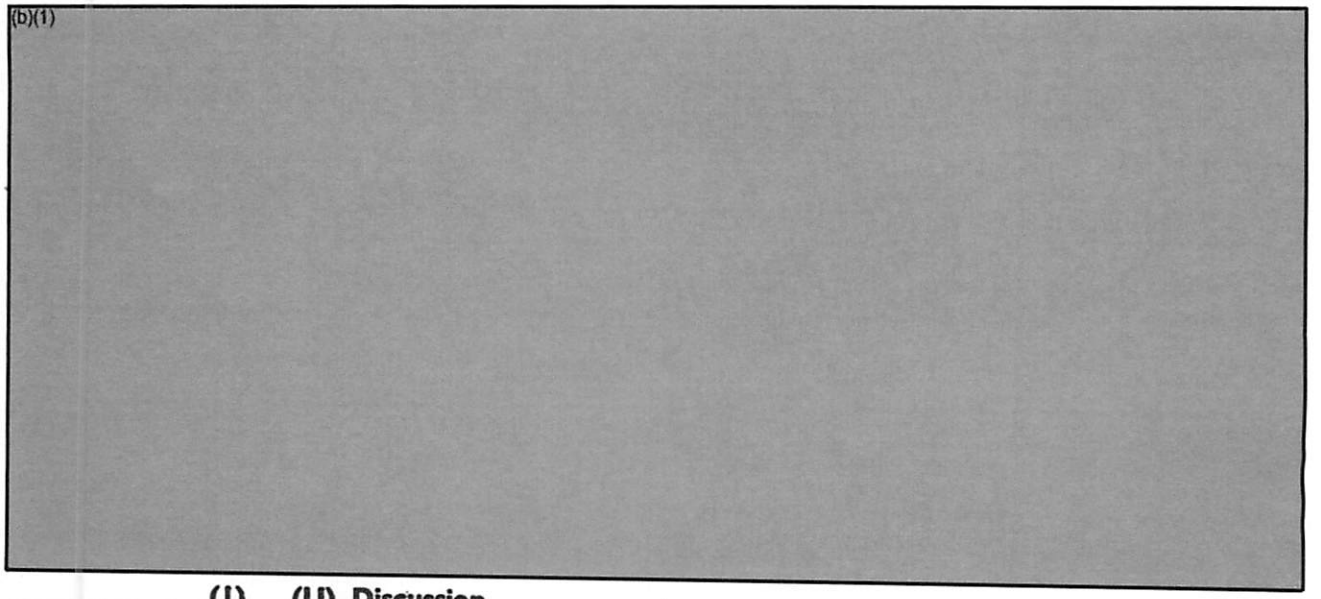


~~SECRET~~

CHAPTER VI

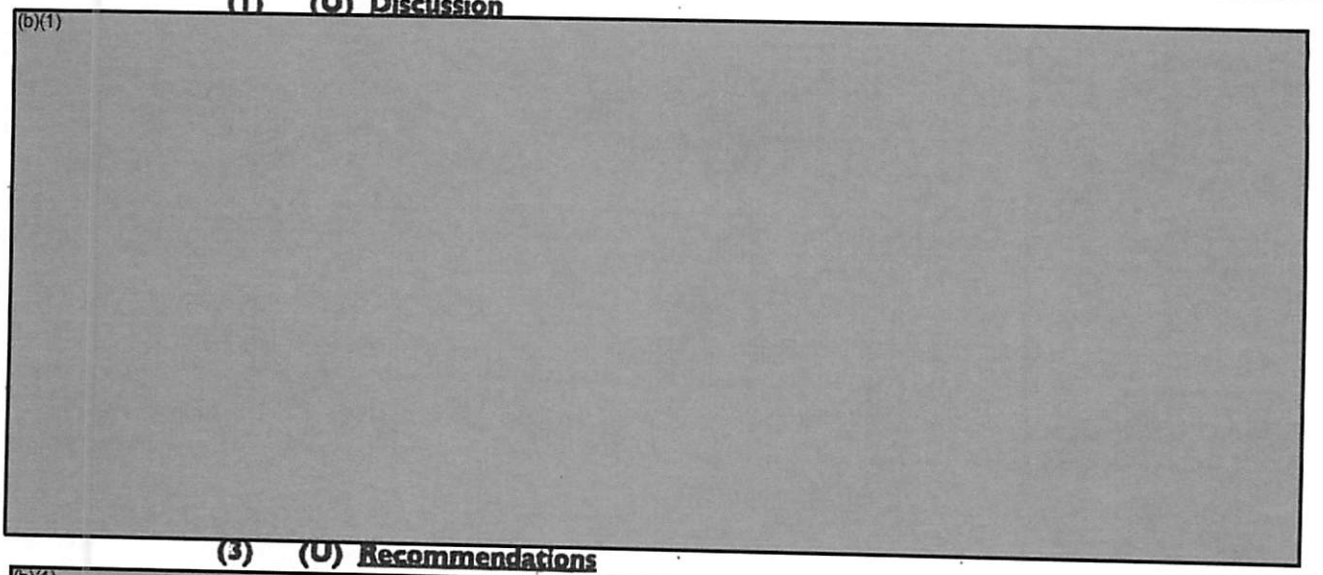
(U) C4I ISSUES

(b)(1)



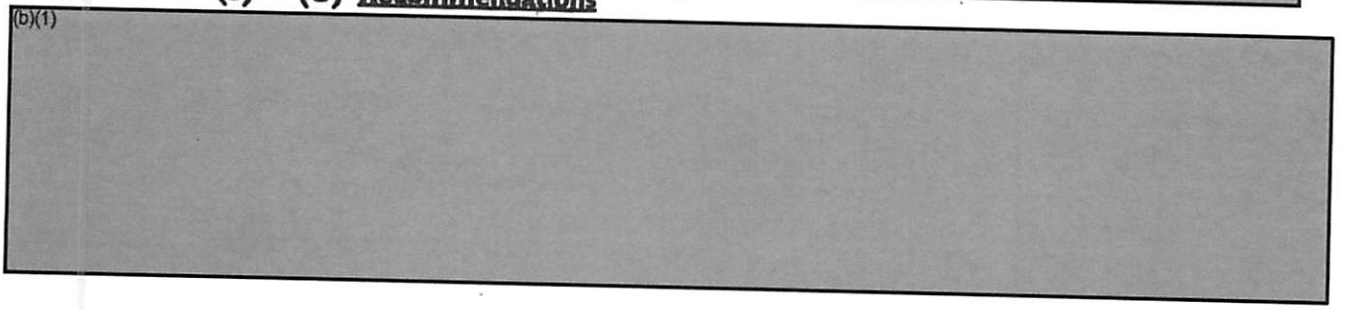
(1) (U) Discussion

(b)(1)



(3) (U) Recommendations

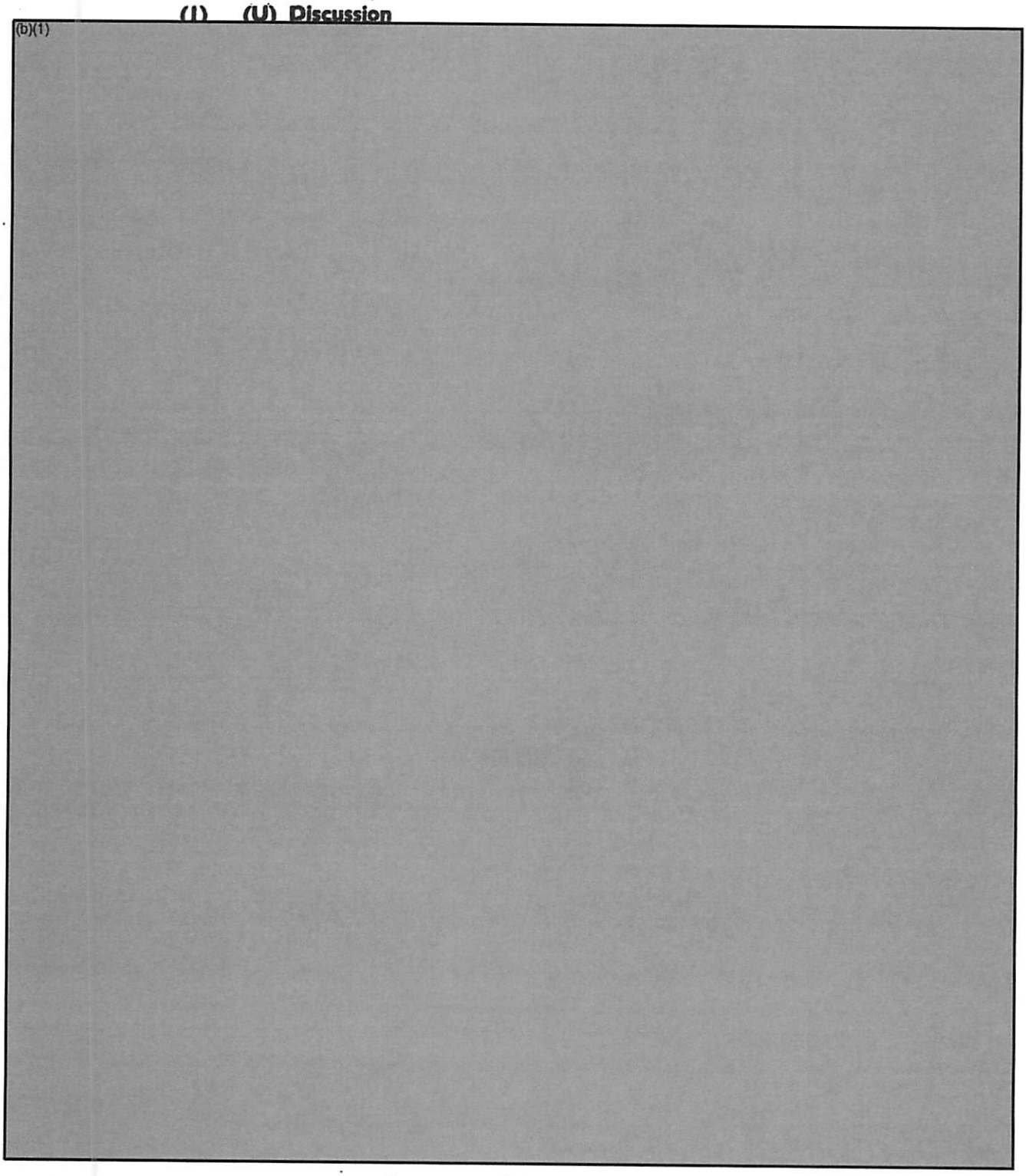
(b)(1)



~~SECRET~~

(I) (U) Discussion

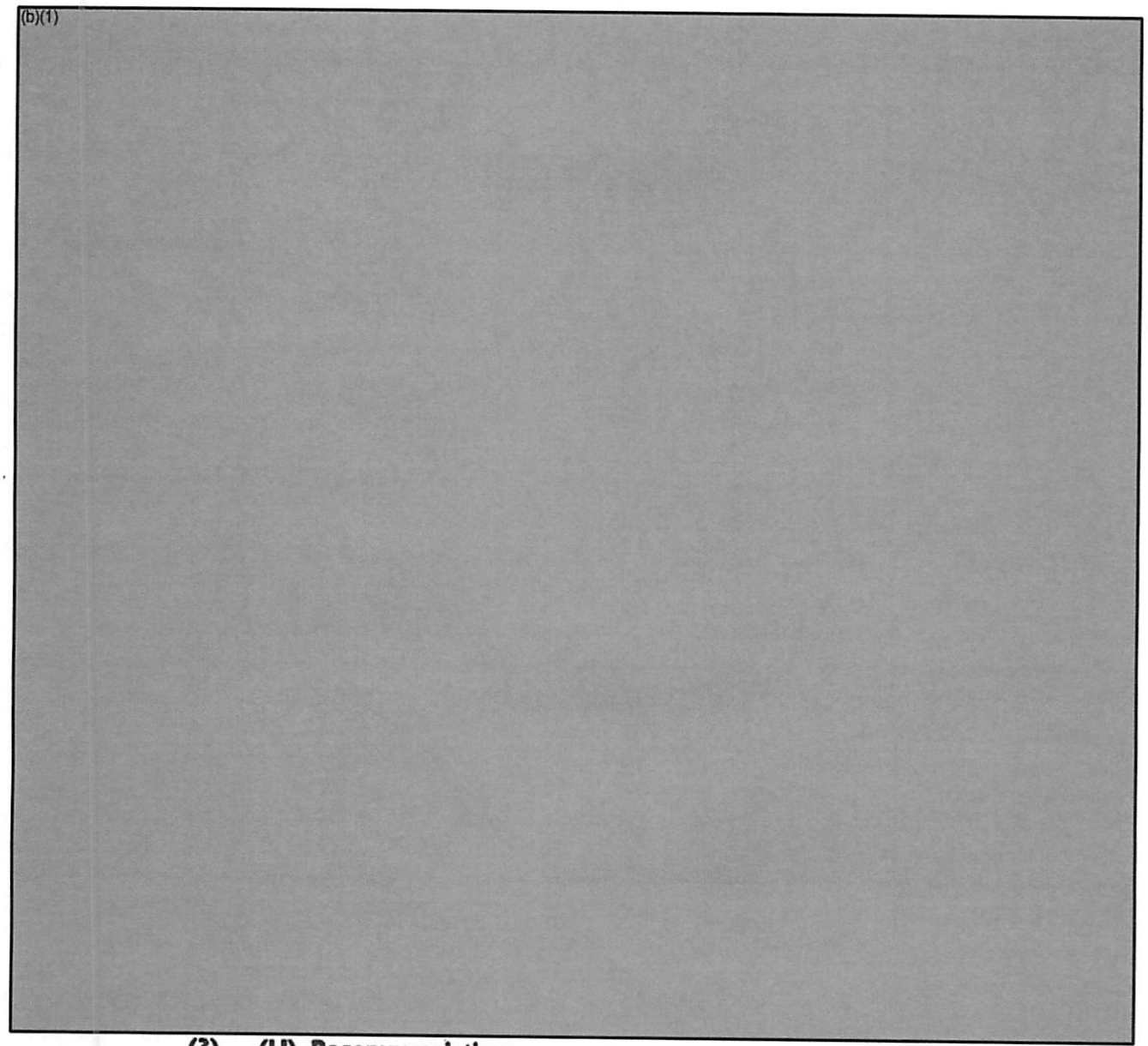
(b)(1)



~~SECRET~~

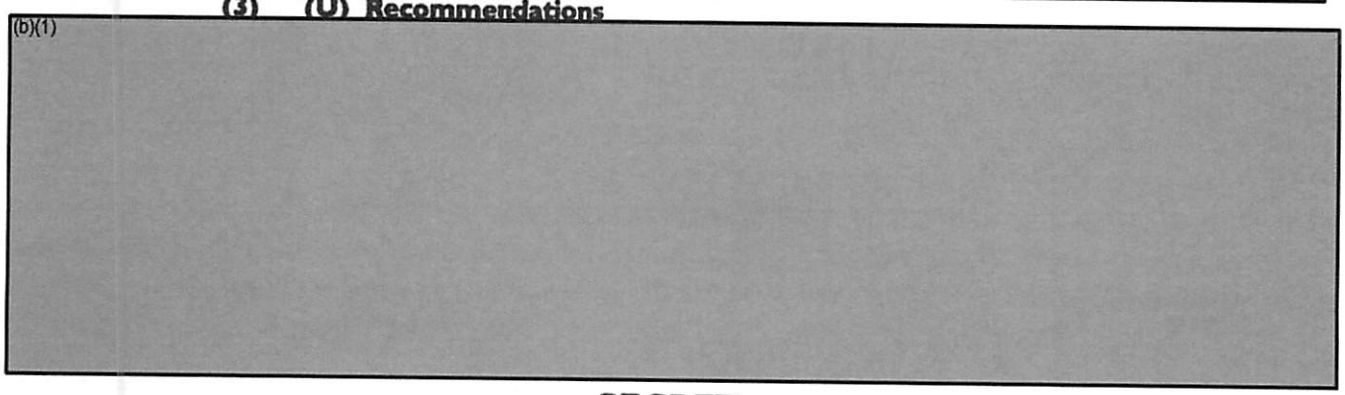
~~SECRET~~

(b)(1)



(3) (U) Recommendations

(b)(1)



~~SECRET~~

(b)(1)

[redacted]

(I) (U) Discussion

(b)(1)

[redacted]

(3) (U) Recommendations

(b)(1)

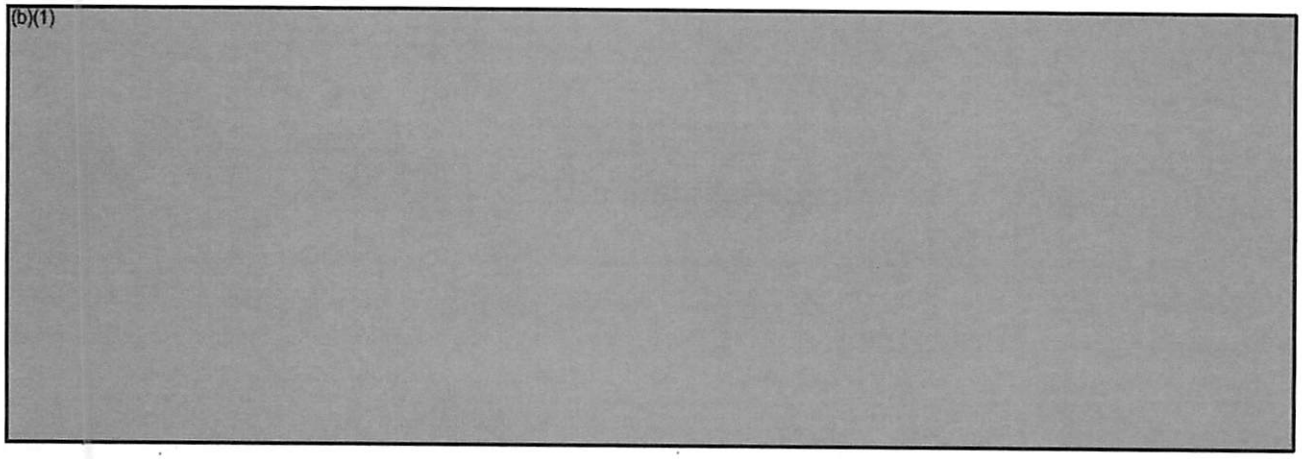
[redacted]

~~SECRET~~

CHAPTER VII

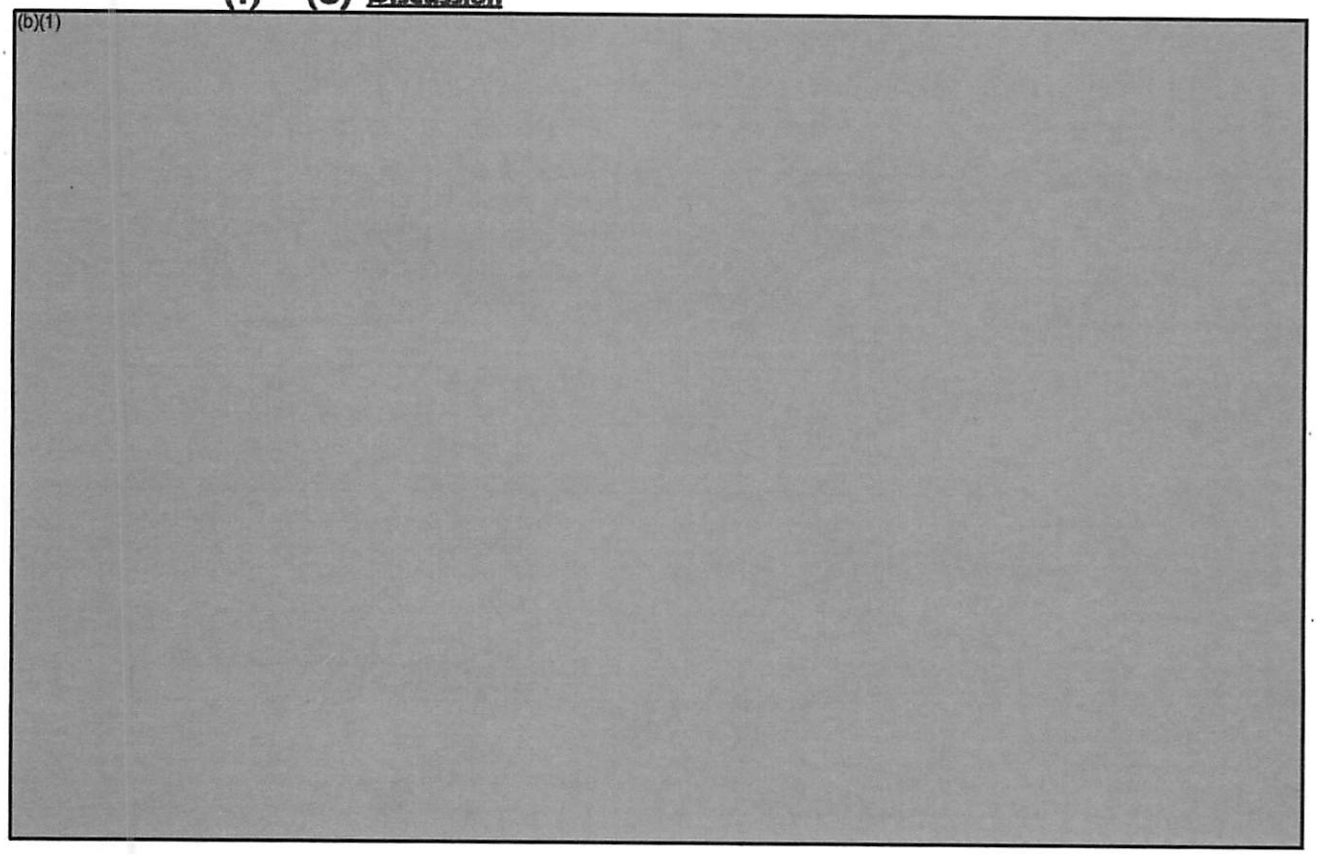
(U) INTELLIGENCE SUPPORT ISSUES

(b)(1)



(I) (U) Discussion

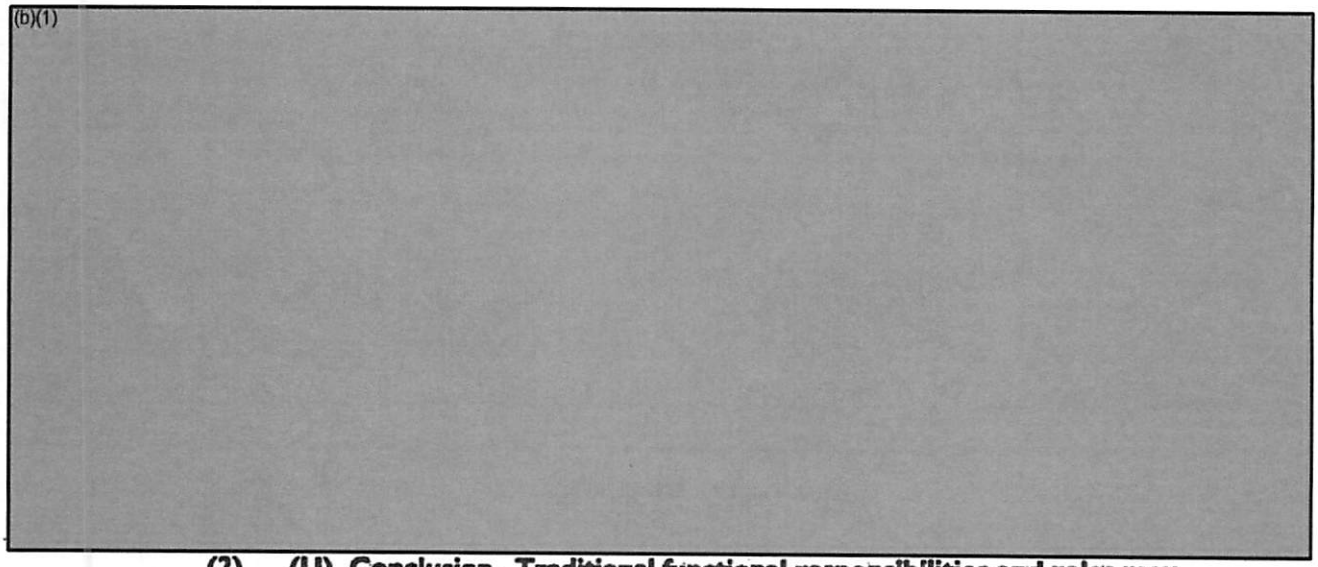
(b)(1)



(I) (U) Discussion

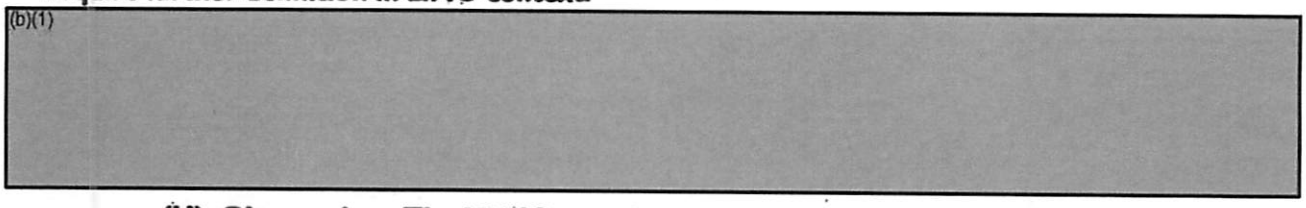
(b)(1)

(b)(1)



(2) (U) Conclusion. Traditional functional responsibilities and roles may require further definition in an IO context.

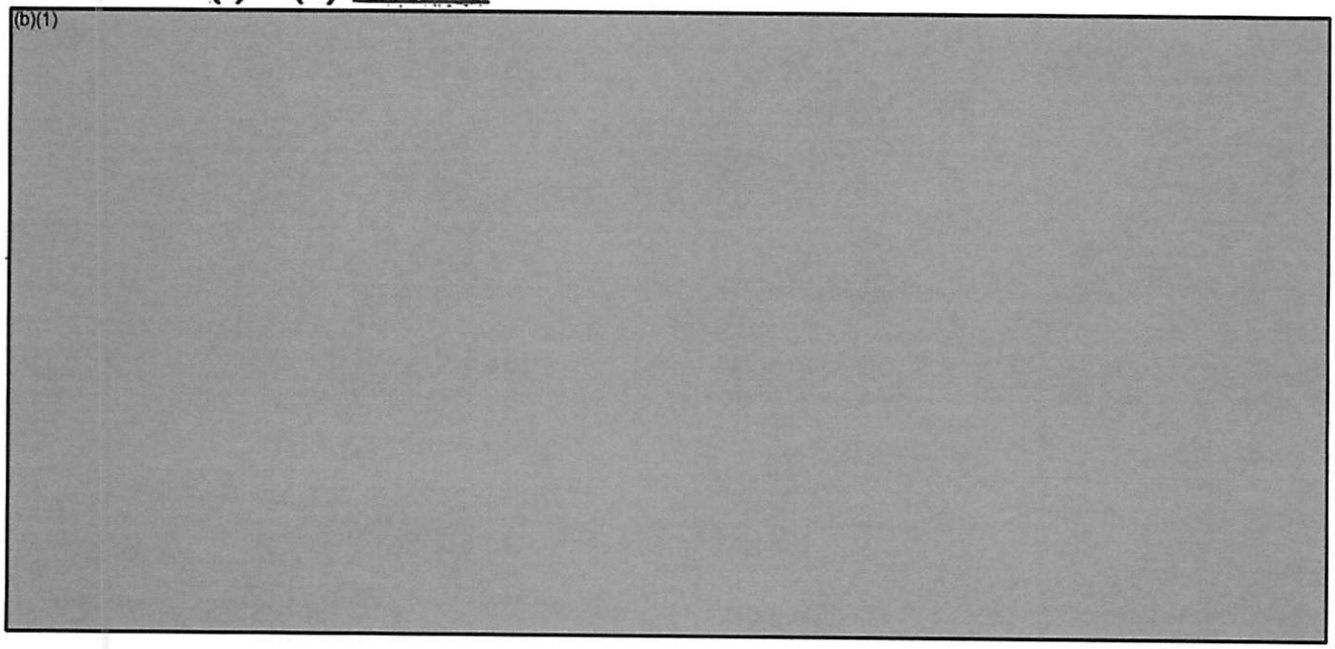
(b)(1)



c. (U) Observation. The NMJIC experimented with various internal Intelligence Working Group configurations for the IO crisis.

(1) (U) Discussion

(b)(1)



~~SECRET~~

(b)(1)

[redacted]

(1) (U) Discussion

(b)(1)

[redacted]

(3) (U) Recommendations

(b)(1)

[redacted]

e. (U) Observation. During ER97-1 the NMJIC found the exchange of LNOs to be invaluable in interpreting information, facilitating the exchange of information, and providing technical advice.

(1) (U) Discussion

(a) (U) An essential element of interagency operations requires a fusion or sharing of critical information and intelligence. A time-honored, comfortable, and effective method to coordinate in a crisis has been the use of LNOs.

(b)(1)

[redacted]

~~SECRET~~

(b)(1)

(c) (U) There were designated points of contact at NSA and the CIA.

(b)(1)

(e) (U) DISA was particularly hit hard with requests for LNOs. Each request essentially cut into the available technical staff used for event analysis.

(f) (U) Some crisis center managers would suggest that the use of LNOs is a quick yet effective fix for voids in interagency standing operating procedures (SOPs). Others would suggest that LNOs are essential, even with technology and processes, to interpret and facilitate.

(g) (U) Agencies and staffs have experienced dramatic downsizing in recent years. The pool of available technically competent manpower has decreased at the same time our electronic data management capability has increased.

(2) (U) Conclusion

(b)(1)

(c) (U) Supporting agencies need to provide liaison teams to the lead agency upon request. As the crisis will not necessarily involve every agency, the lead agency needs to identify those supporting agencies from which it needs assistance. The liaison teams provide the lead agency a single point of contact for support as well as keep the supporting agencies informed of the operation.

(b)(1)

(l) (U) Discussion

(a) (U) J-39 established a watch cell called the Information Response Cell (IRC).

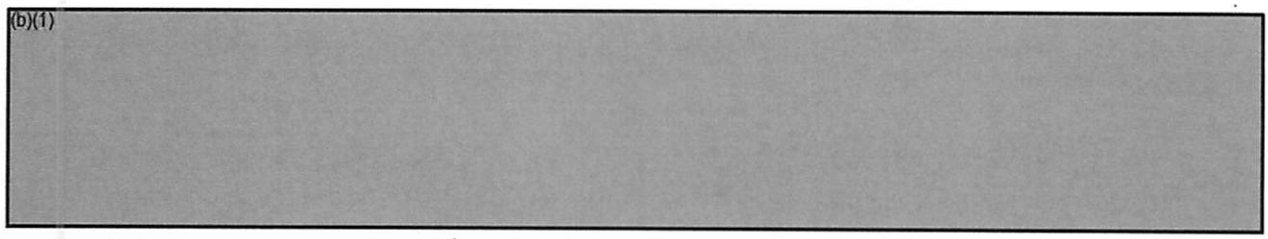
(b)(1)

(c) (U) Initially, intelligence sharing between these cells was problematic. A NMJIC representative was assigned to the J-39 24-hours a day; however, the IRC was not getting the necessary messages due to improper message addressing.

(b)(1)

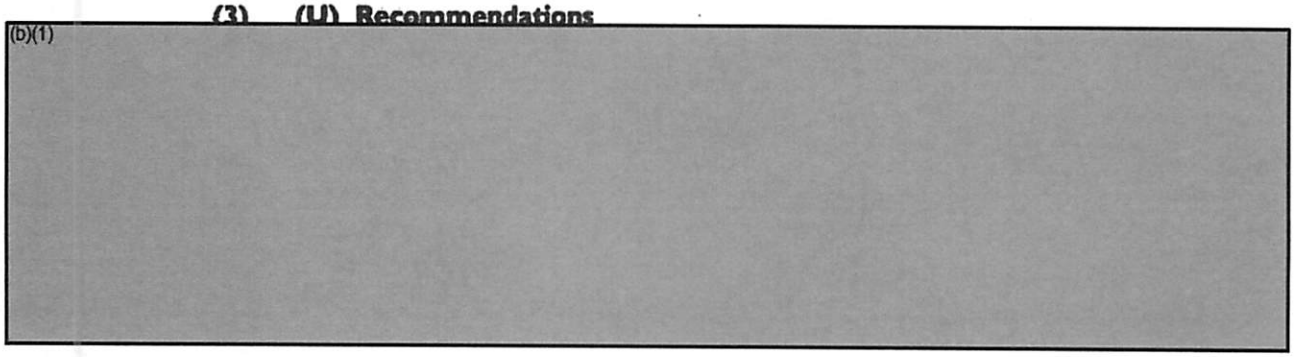
~~SECRET~~

(b)(1)



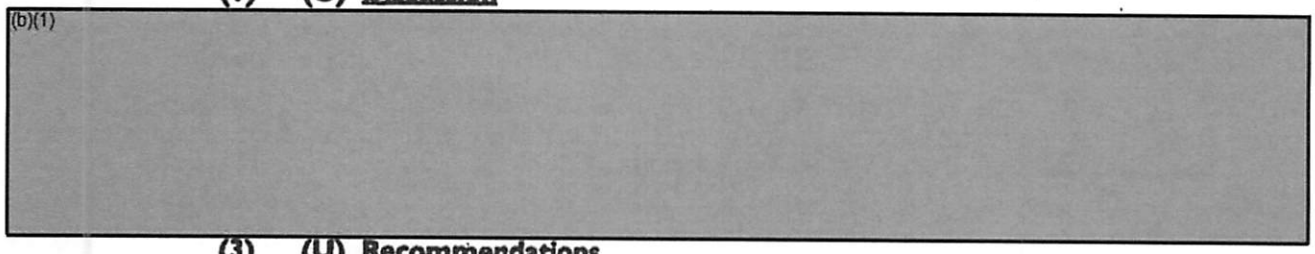
(3) (U) Recommendations

(b)(1)



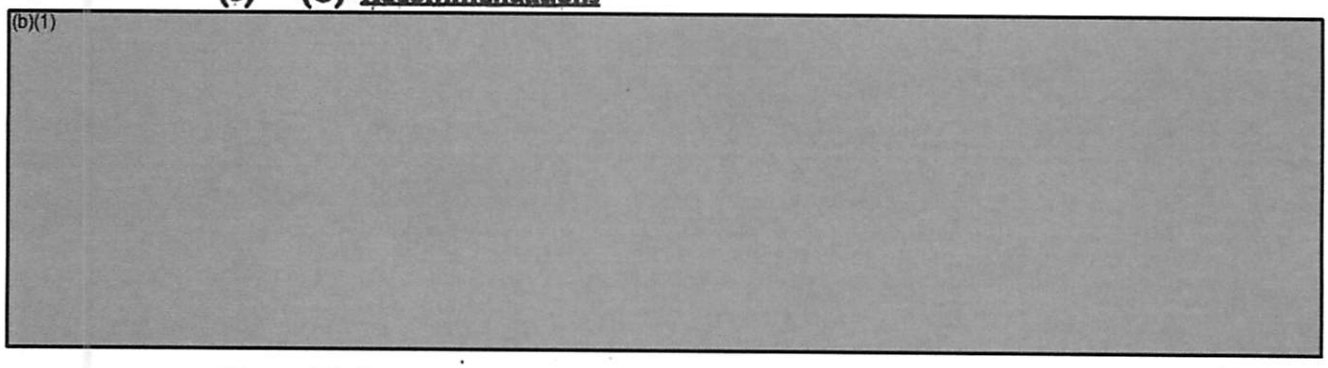
(I) (U) Discussion

(b)(1)



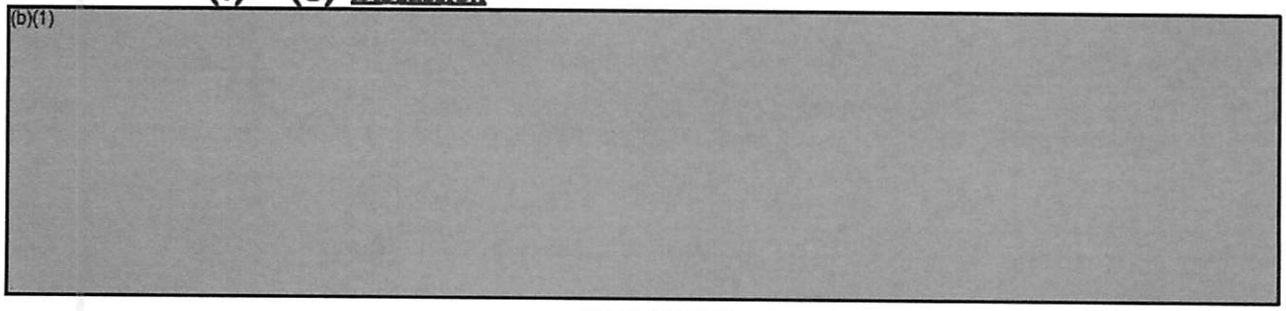
(3) (U) Recommendations

(b)(1)



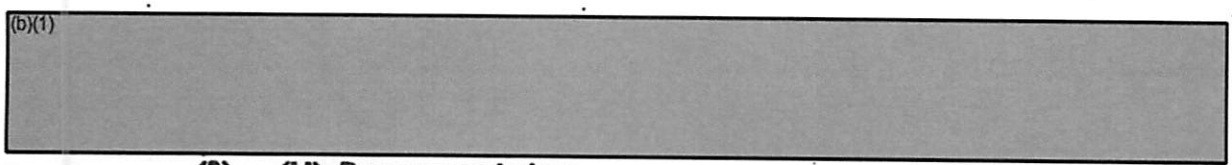
(I) (U) Discussion

(b)(1)



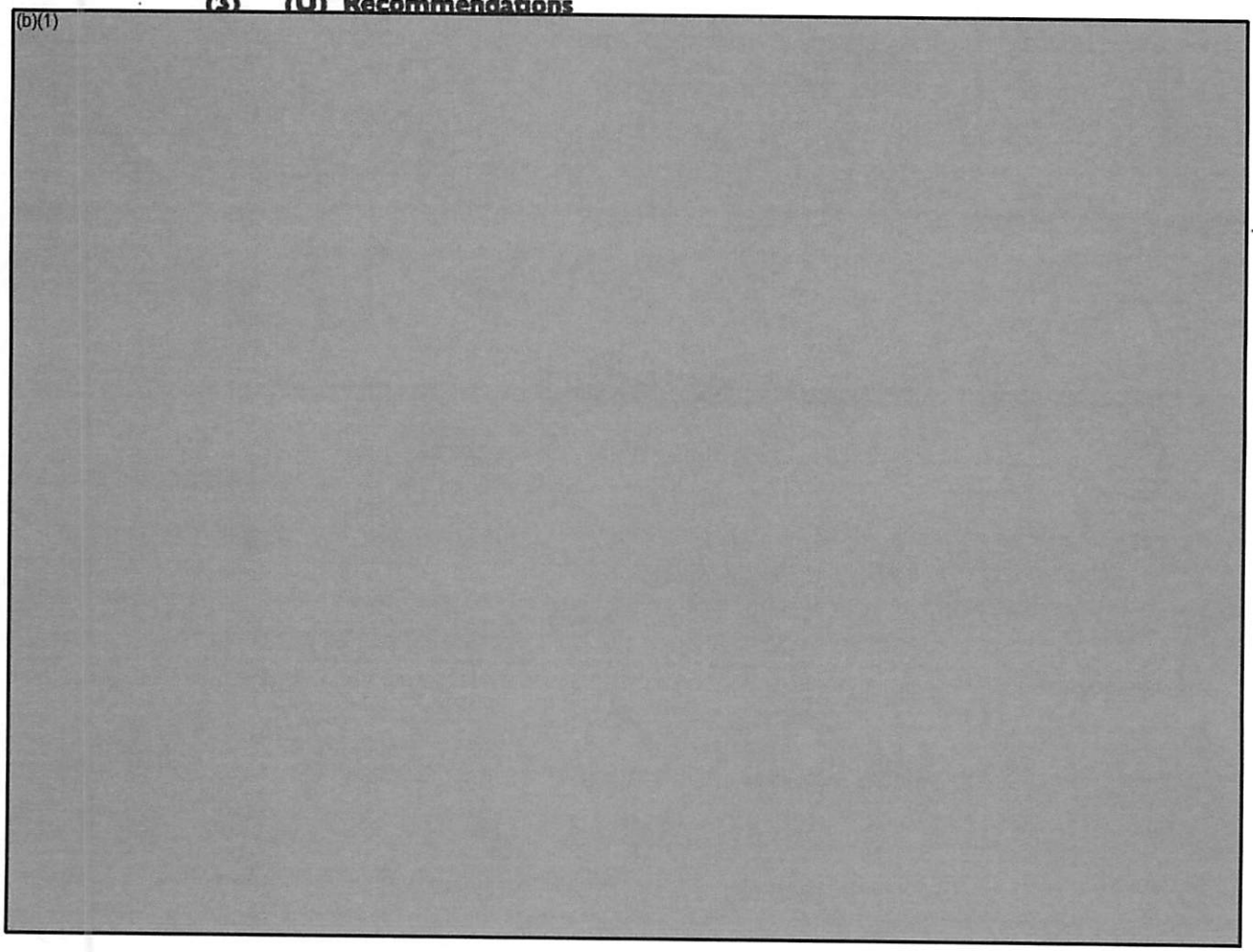
~~SECRET~~

(b)(1)



(3) (U) Recommendations

(b)(1)

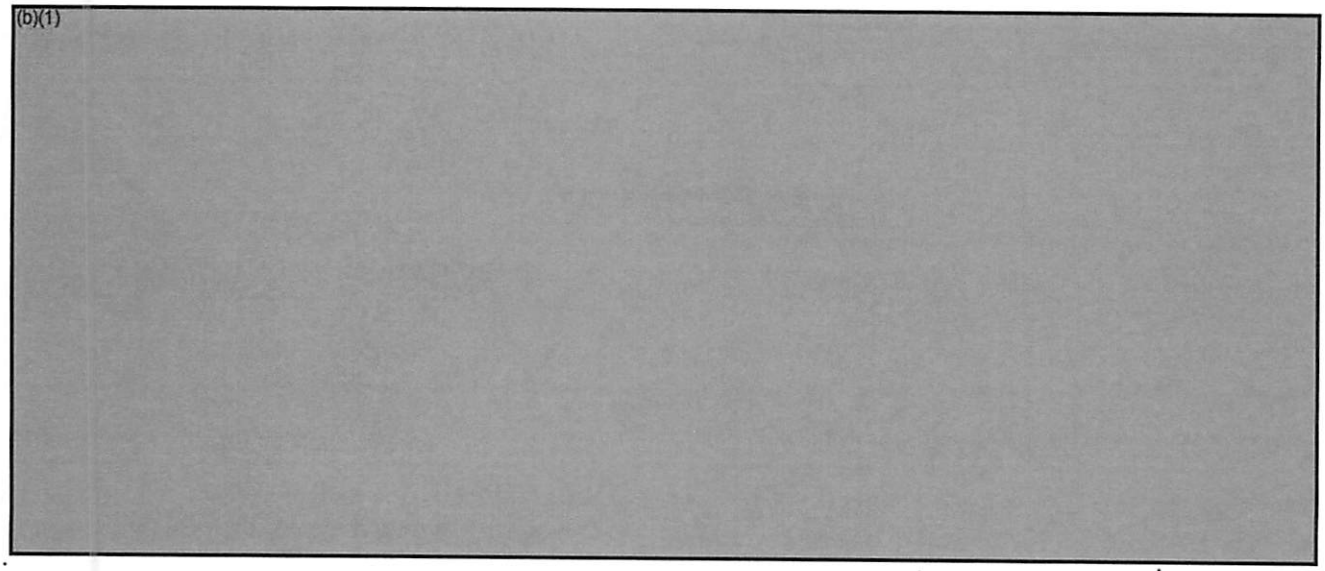


(INTENTIONALLY LEFT BLANK)

CHAPTER VIII

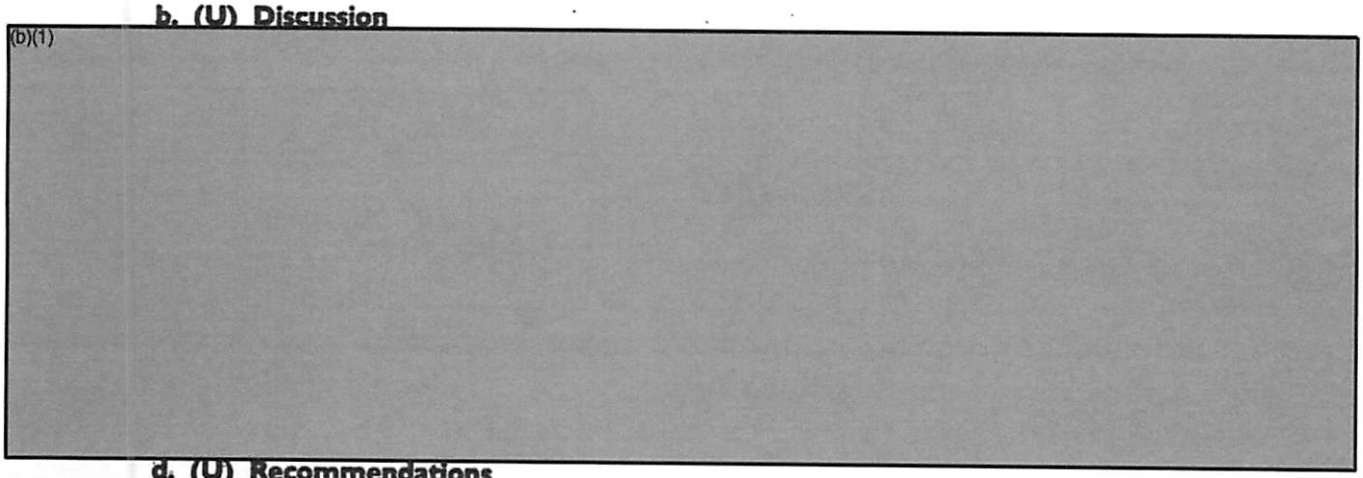
(U) LEGAL ISSUES

(b)(1)



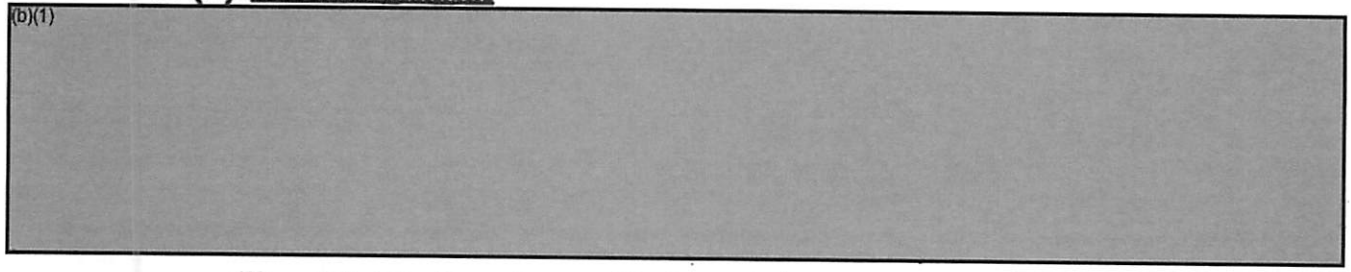
b. (U) Discussion

(b)(1)



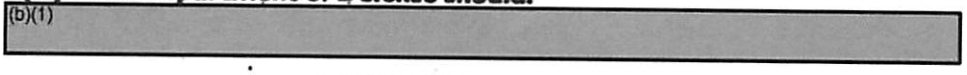
d. (U) Recommendations

(b)(1)



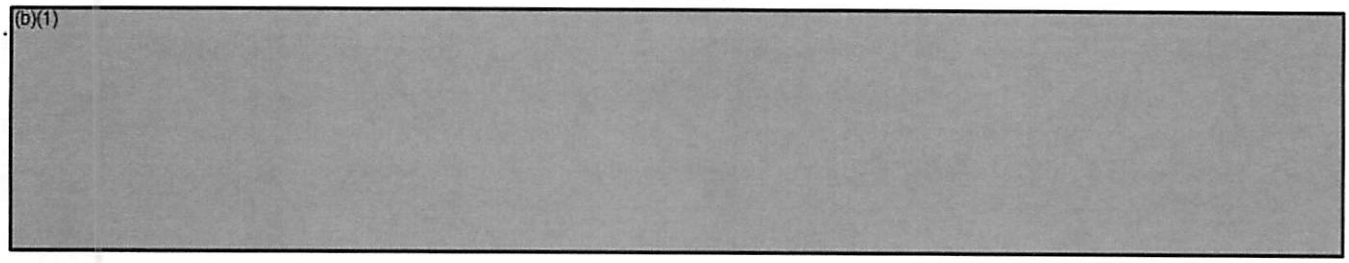
(2) (U) The Department of Defense should:

(b)(1)



~~SECRET~~

(b)(1)



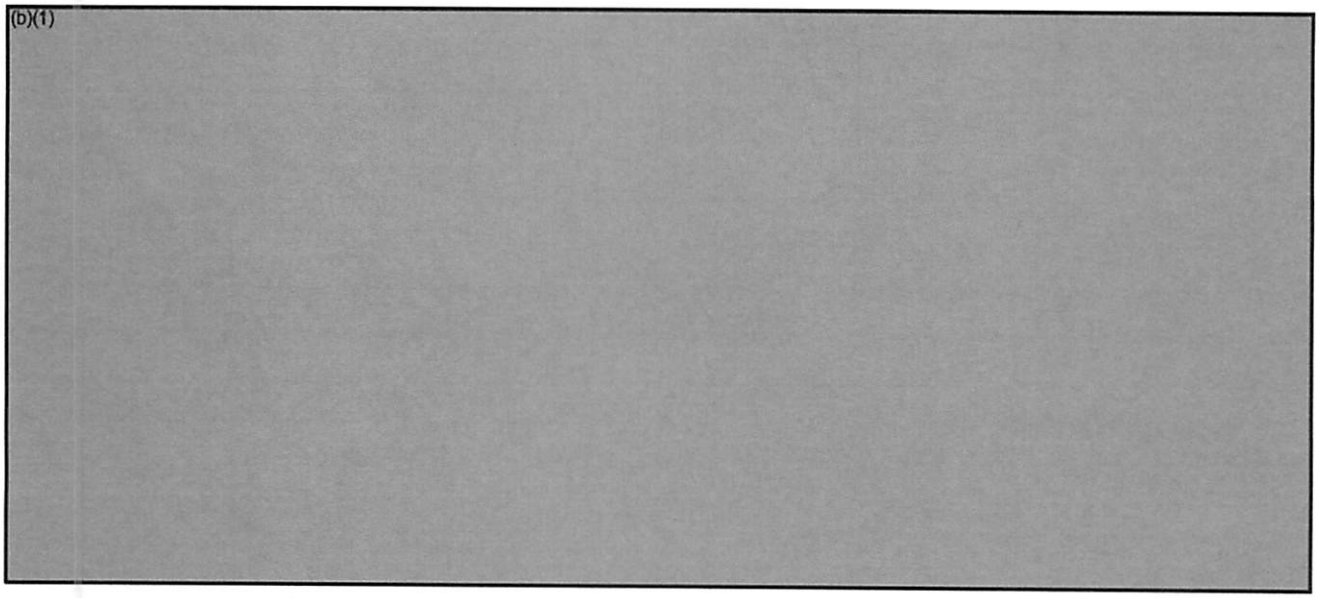
(INTENTIONALLY BLANK)

~~SECRET~~

CHAPTER IX

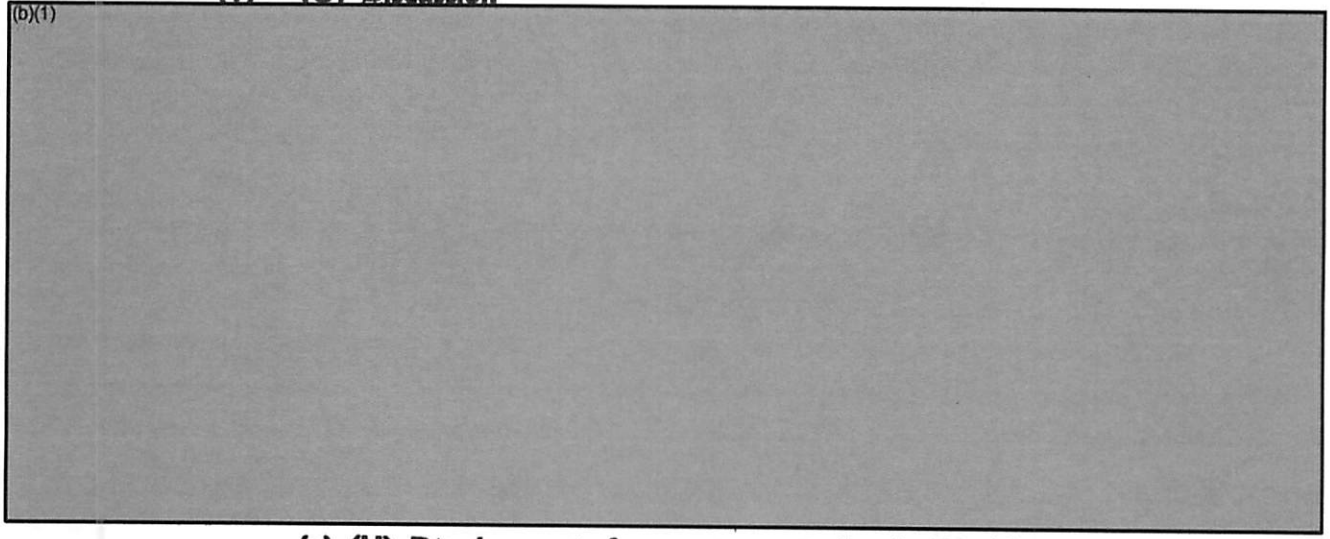
(U) PA POLICY AND STRATEGY ISSUES

(b)(1)



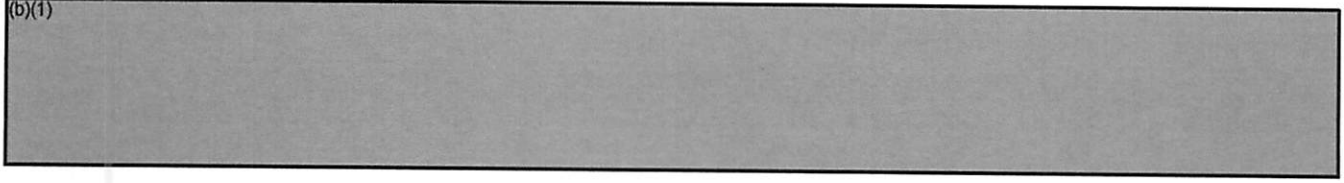
(1) (U) Discussion

(b)(1)



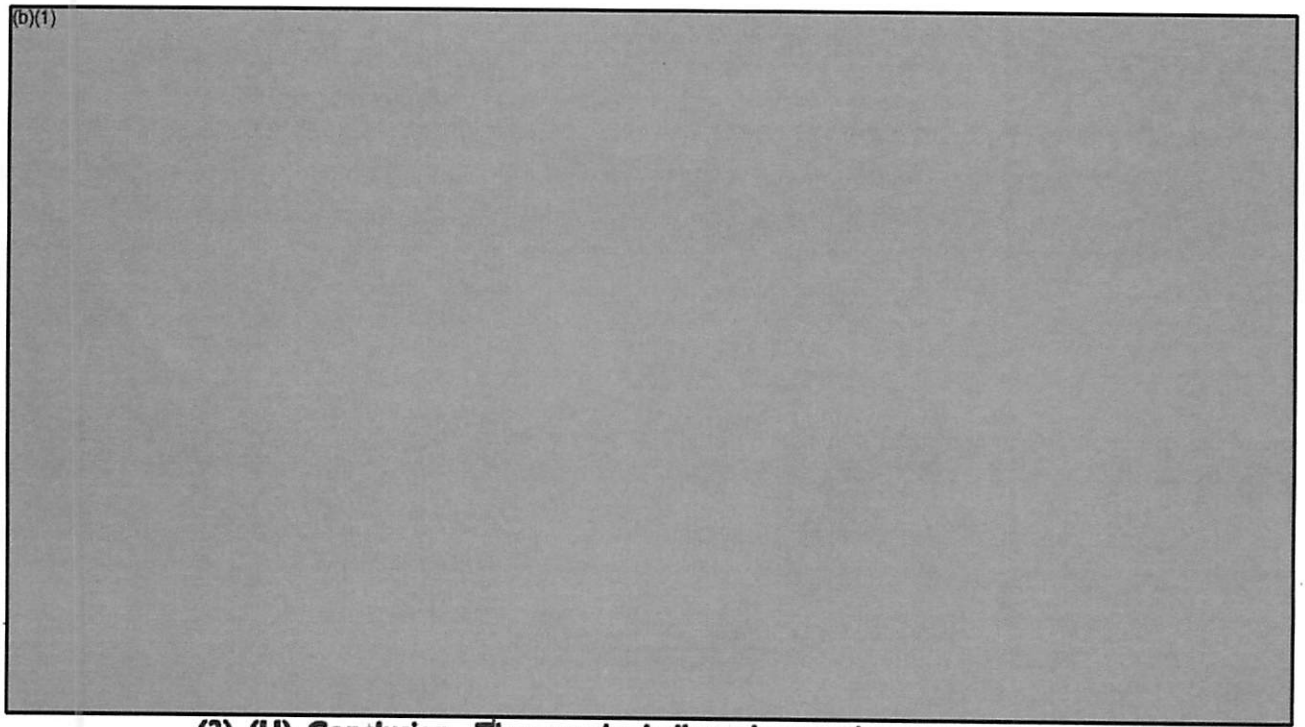
(e) (U) Development of press comments for the President was discussed and tasked to the lead agency (the Federal Bureau of Investigation); however, the FBI does not normally prepare these types of comments.

(b)(1)



~~SECRET~~

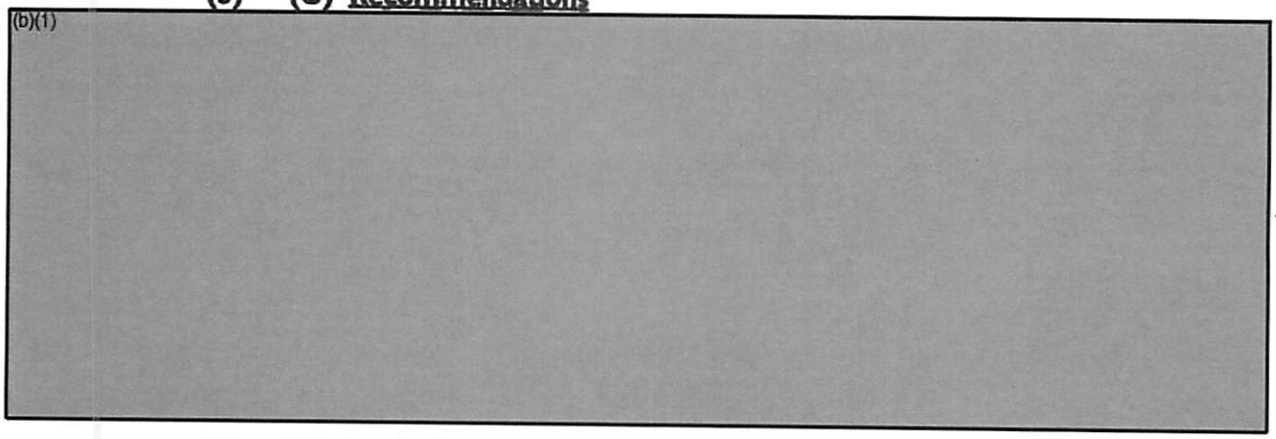
(b)(1)



(2) (U) Conclusion. The exercise indicated a reactive posture to events from PA and PSYOP proponents. The themes for dealing with the situation and future actions were not being developed rapidly enough to keep up with events. The exercise also demonstrated the need for balance among PA, PSYOP, and operations security (OPSEC).

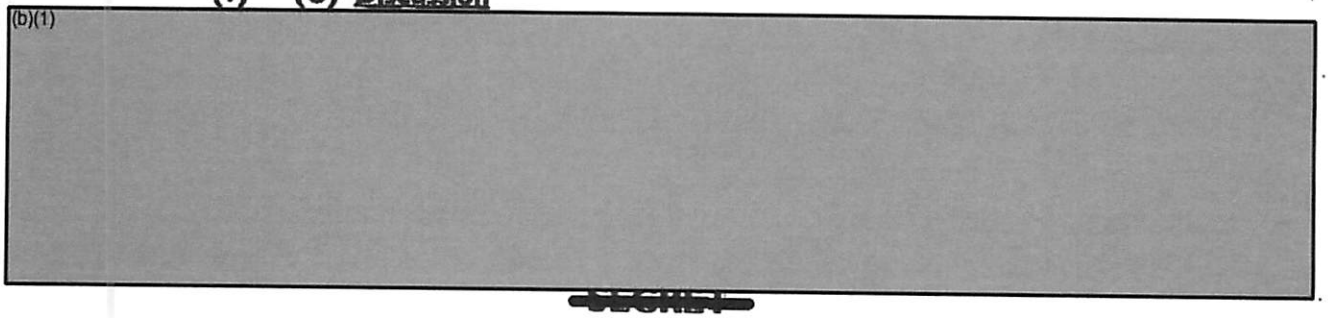
(3) (U) Recommendations

(b)(1)



(I) (U) Discussion

(b)(1)



~~SECRET~~

~~SECRET~~

(b)(1)

[redacted]

(3) (U) Recommendations

(b)(1)

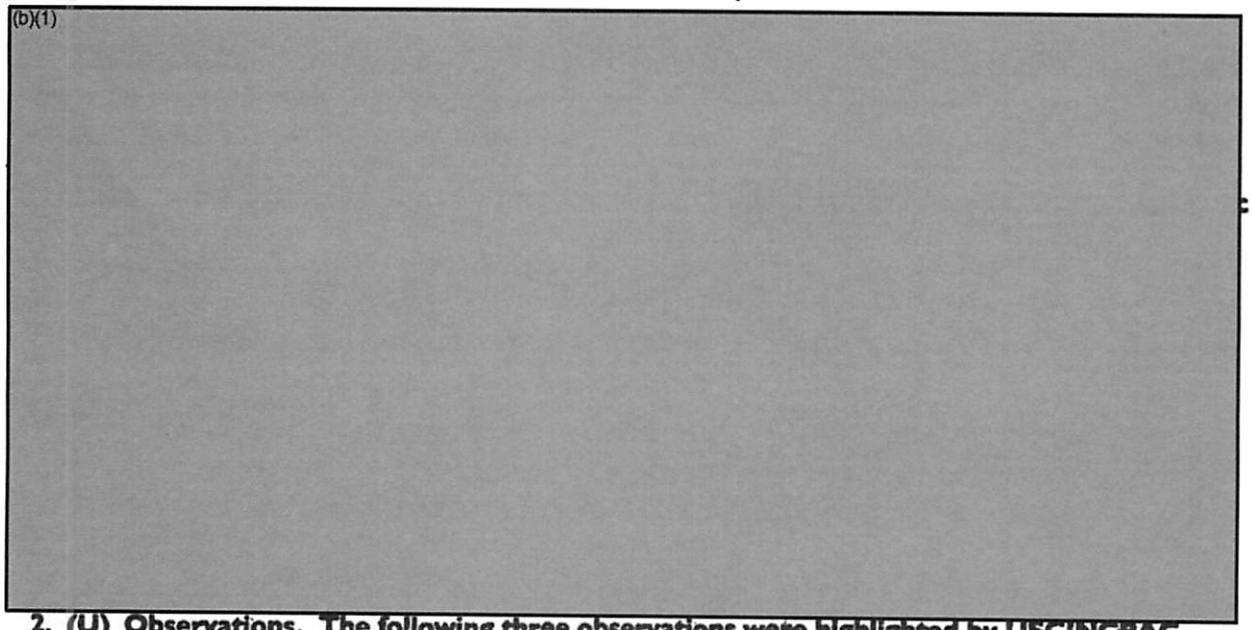
[redacted]

(INTENTIONALLY BLANK)

CHAPTER X

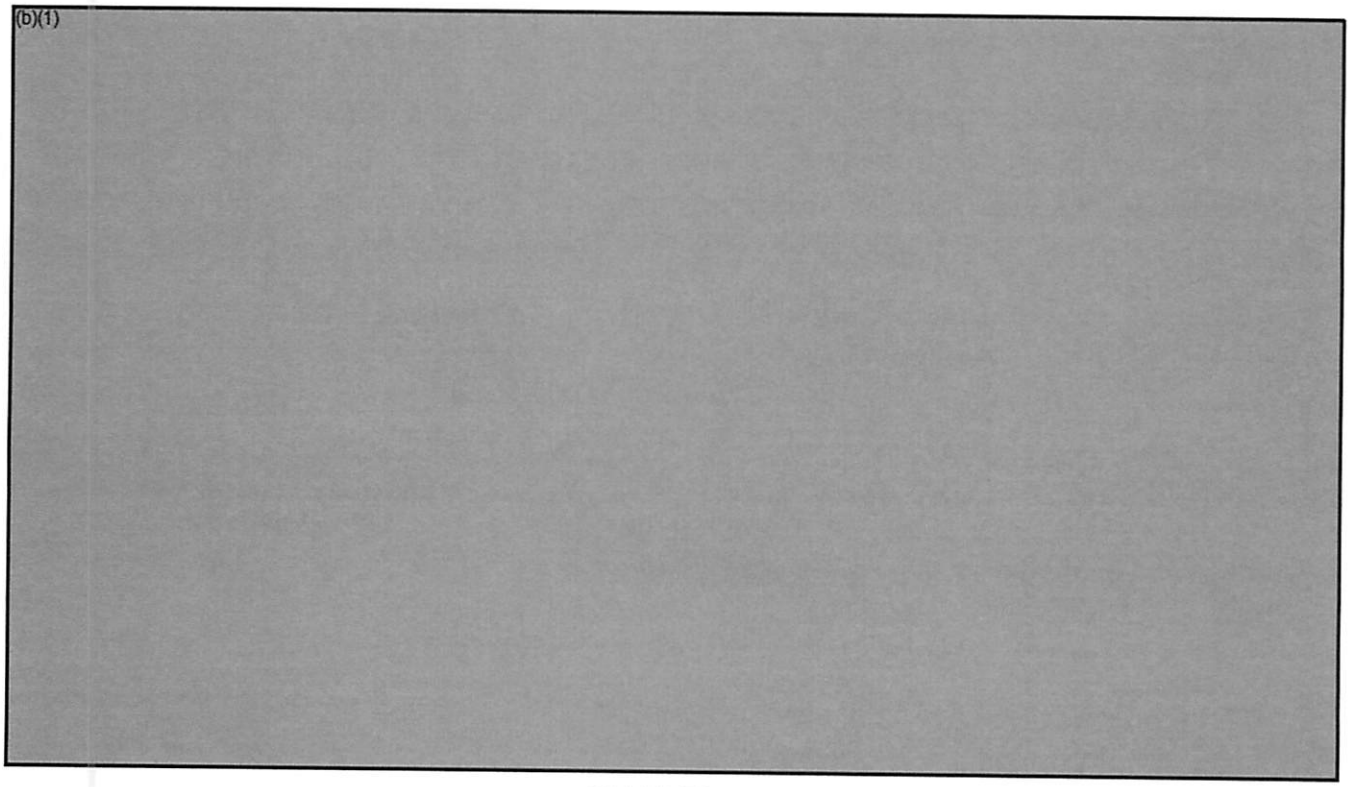
(U) USPACOM OBSERVATIONS

(b)(1)



2. (U) Observations. The following three observations were highlighted by USCINCPAC during ER97-1.

(b)(1)



~~SECRET~~

(b)(1)

[redacted]

(U) Discussion

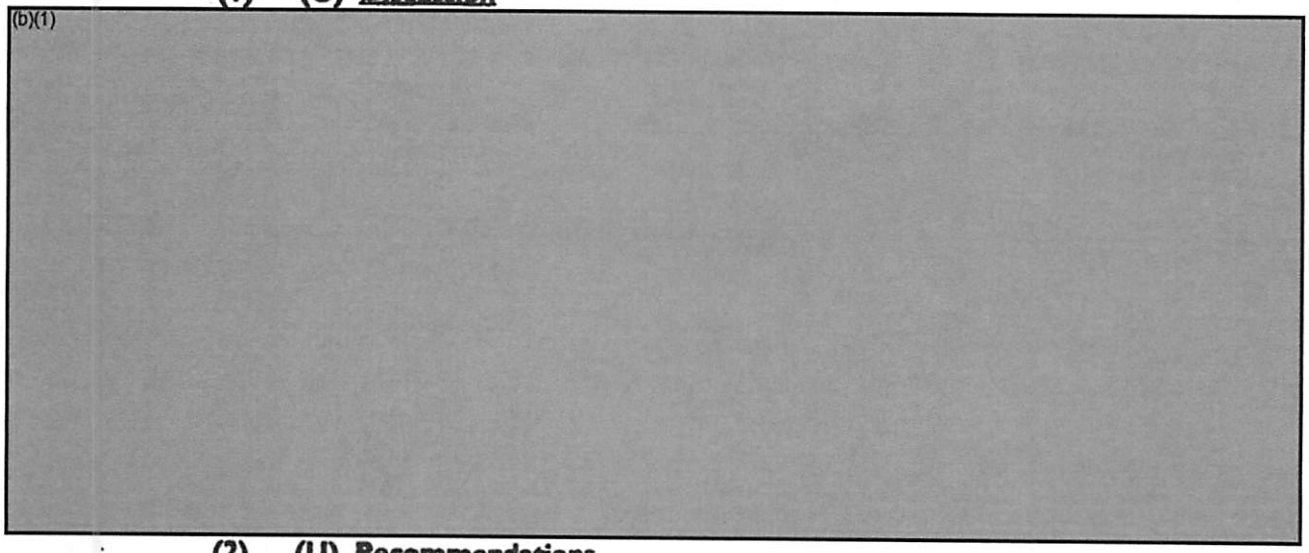
(b)(1)

[redacted]

~~SECRET~~

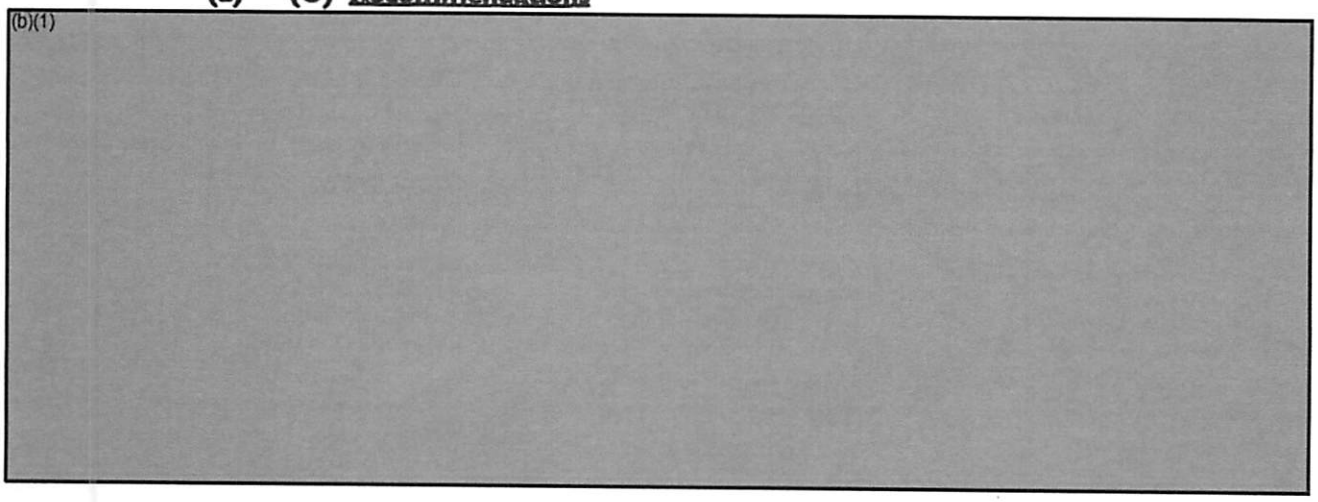
(1) (U) Discussion

(b)(1)



(2) (U) Recommendations

(b)(1)



CHAPTER XI

(U) OTHER OBSERVATIONS

1. (U) Introduction

a. (U) This exercise was the first serious cyber war for most in the Department of Defense and the Government Interagency Community. Unlike most exercises that are designed to train and also to evaluate established plans, policies, and procedures, this exercise clearly demonstrated that Information Operations (IO) plans, policies, and procedures are still very much in the formative stage of development.

b. (U) As a result, the most notable observation from this exercise was that it raised more questions than it answered. People know what needs to be done; however, who or what organization should do it? How do we detect intrusions? Who reports to whom and in what format is it reported? The questions are many, but to ensure the essence of the uncertainty is not lost in these pages, the most commonly observed uncertainties are included in this chapter. Some questions reflect a lack of policy or lack of knowledge of the existing policy or the implementing procedures; and some questions reflect contradictions within and among agencies.

2. (U) Observations. The following list is a summation of questions and concerns raised by participants during Exercise ELIGIBLE RECEIVER 97-1 (ER97-1). This list does not attempt to be all inclusive but, instead, a representative of a week of close observation. For convenience, the questions coincide with the chapters in this report.

a. (U) Chapter II. Awareness and Understanding

(1) (U) Is there a shortage of trained information operations (IO) specialists?

(2) (U) Is the peacetime manning level of IO specialists sufficient to meet the demands for additional analysts, liaison personnel, and augmentees in a crisis operation?

(3) (U) Is the potential problem in manning the technical skilled positions shortfall the result of too much overlap in responsibilities among the various organizations?

(b)(1)

[redacted]

(5) (U) What is the role of either the US Atlantic Command or Forces Command for critical asset protection of the NII, and is this role active or passive?

(6) (U) How should industry be involved in developing infrastructure protection responsibilities and procedures?

(7) (U) Is there a decision support structure that would provide unity of effort in dealing with infrastructure attacks?

(8) (U) Are there any required advanced training and education programs for system administrators within the Department of Defense?

(9) (U) Where are the IO reporting requirements codified?

(10) (U) Should we not be able to find some real IO talents in the National Guard and Reserve?

(b)(1)

[redacted]

~~SECRET~~

(12) (U) How do we educate people about reporting procedures and the need to be sensitive that computer- or telecommunication-related problems may be indicative of hostile intent and not accidental?

b. (U) Chapter III. Policy Issues

(b)(1)

(3) (U) How do we draw the line between widespread criminal activity and a coordinated strategic attack against the United States?

(4) (U) By what mechanisms would authorities be transferred from law enforcement to the National Security Community?

c. (U) Chapter IV. Interagency Coordination Issues

(b)(1)

(2) (U) Should we talk to industry now about fixing identified weakness?

(3) (U) Was the interagency or IPTF able to distinguish what may appear to be an insignificant problem for one infrastructure (e.g., electric power) but may have substantial consequences when looked at from the perspective of another infrastructure?

(4) (U) Should lead-agency jurisdiction depend on the identity and location of the perpetrators, site of initiation, or end-result site of attacks?

(5) (U) Is it reasonable that lead-agency responsibilities would shift with a changing scenario, and, if so, how do fusion cells respond procedurally to the shift?

(6) (U) Does the Department of Defense need to have a closer real-world relationship with the Federal Bureau of Investigation (FBI) on sharing low-level intrusion information?

(7) (U) What should be the working relationship in the Joint Staff between J-39 and the IO Task Force?

(b)(1)

(9) (U) What is the time and content requirement for attack assessments to make them usable products in a crisis?

(10) (U) Should the designated lead agency be provided with standard guidelines of minimum expectations and authorities to facilitate its potentially directive efforts over other agencies?

(b)(1)

(12) (U) When should the private sector be informed that an IO attack is occurring?

~~SECRET~~

(13) (U) What are the legal aspects of warning or not warning the private sector?

(b)(1)

[redacted]

d. (U) Chapter V. Planning, Procedures, and Processes Issues

(1) (U) Which crisis command centers or agencies need to have IO crisis action standing operating procedures (SOPs) for IO?

(2) (U) Since each node is a potential intrusion point, should all agencies be required to have an IO SOP?

(3) (U) What are the essential elements of information required by a command center during an IO crisis?

(4) (U) Should a Consequence Management (CM) Team be incorporated into SOPs since this function is often overlooked for IO, weapons of mass destruction, and terrorism?

(b)(1)

[redacted]

(8) (U) Is there a way to reduce the amount of time it takes to rekey many STU systems?

(9) (U) In the alerts or warnings, when does the Government request industrial cooperation versus direct compliance for increased defensive measures?

(10) (U) In the alerts or warnings, who would be liable for unforeseen problems?

(b)(1)

[redacted]

(12) (U) In the alerts or warnings, what feedback from industry is desired; in what format; to whom; and how frequent, if at all?

(13) (U) In the alerts or warnings area of concern, is it practical to have an on-the-shelf comprehensive plan for public and industrial alerts with details of how, by whom, to whom, the legal basis, existing Presidential authorities, potential authorities to request, reporting requirements, and responsibility for data analysis?

(14) (U) Can systems and procedures designed to detect intrusion have their trigger thresholds lowered to thwart intrusions demonstrated in the exercise?

(b)(1)

[redacted]

(16) (U) Was the lack of intrusion reporting due to inadequate detection, exercise

design, lack of certain organizations being involved, or systemic problems?

(17) (U) Is there a reporting system or protocol from the Service Computer Emergency Response Teams (CERTs) to DISA?

(18) (U) Do reporting procedures distinguish between normal and crisis reporting procedures?

(19) (U) Who will coordinate the review of potential Service shortfalls in intrusion-detection programs?

(20) (U) Should military warning order templates have IO sections alerting CINCs to types of IO attacks and protective measures?

(21) (U) How do we get crisis cells dedicated to CM or future operations to be institutionalized in DOD and interagency crisis action planning?

e. (U) Chapter VI. C4I Issues

(b)(1)

(5) (U) What are the implications for hardware acquisition and system architecture?

(6) (U) Can we extrapolate the exercise results to assess how vulnerable the rest of the DOD command, control, and communications (C3) links actually would be if subjected to similar attacks?

(b)(1)

f. (U) Chapter VII. Intelligence Support Issues

(1) (U) What are the data fusion requirements for IO offensive and defensive operations?

(2) (U) How do you efficiently coordinate the roles of J-3, who is concerned about the loss of information systems and impact on forces; J-2, who is responsible for determining threats to the systems; and J-6, who responsible for providing network services?

(b)(1)

(4) (U) What was the mechanism, other than using telephone calls, for sharing

intelligence among the agencies?

(5) (U) What is the utility of J-39, which has approximately 5 percent of its work in compartmented areas, spending 100 percent of its time during a crisis segregated from the main Crisis Response Team?

(6) (U) Is there any correlation between Defense Readiness Conditions (DEFCONs) and IO Threat Conditions (THREATCONs)?

(b)(1)

[redacted]

(8) (U) Should attack assessments be a NMJIC product, a J-3 product, or a product of a Federal agency?

g. (U) Chapter VIII. Legal Issues

(1) (U) What different authorities are needed to respond to threats in the continental United States (CONUS) versus outside the continental United States (OCONUS)?

(2) (U) What authorities would be needed to employ IO tools for defense or counterattack in CONUS or OCONUS?

(3) (U) What is the best national policy or decisionmaking forum to initiate military planning and involvement in IO?

(4) (U) What should be the limits of the DOD role in infrastructure protection or IO defense of the private sector, and would any of these limitations stand up in the face of the public outcry that would accompany disruptions like those in the exercise?

h. (U) Chapter IX. PA Policy and Strategy Issues

(1) (U) Who is responsible for coordinating a national press policy or guidance in an IO event?

(2) (U) Who is responsible for coordinating the public affairs (PA), psychological operations (PYSOP), and OPSEC efforts?

(3) (U) What are the PA office coordination procedures within the Department of Defense down to the field command level, and are they thorough enough to deal with complex fast-moving IO events?

(b)(1)

[redacted]

(5) (U) Why is it that in most exercises we cannot get the PA office to play a greater role, and the topic is always notionalized away?

CHAPTER XII
(U) CJCS JMETL TRAINING

1. (U) General. The CJCS Joint Mission Essential Task List (JMETL) was approved by Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3500.02A, Joint Training Master Plan, 1 October 1995. For Exercise ELIGIBLE RECEIVER 97-1 (ER97-1), planners used the JMETL Strategic-Level National Military Tasks (SNs) to develop the exercise objectives. Based on a review of the exercise concept and CJCS-approved scenario, supporting SNs were selected as training tasks for the Joint Staff.

2. (U) JMETL Training. ER97-1 provided the opportunity for the Joint Staff to train on the following CJCS Joint Mission Essential Tasks (JMETs), which were selected from the Universal Joint Task List (UJTL):

a. (U) SN 2 Develop Strategic Intelligence, Surveillance, and Reconnaissance. To produce the intelligence required by strategic consumers for formulating national-level policy, strategy, and military plans and operations. The strategic intelligence task applies across the range of military operations, including military operations other than war. This task includes providing national strategic surveillance and reconnaissance. (JP 2-0, 3-07.4 (*JP 3-11*))

b. (U) SN 2.2.1 Collect Information on Strategic Situation Worldwide. To obtain information and data from all sources on the strategic situation. Areas of interest include activities and situations that could impact US national security interests and objectives, multinational and regional relations, or US and allied military forces. Of particular importance is information relating to enemy or potential enemys strategic vulnerabilities; strategic forces; strategic centers of gravity; and nuclear, biological, and chemical (NBC) capabilities. This task includes collecting information on key foreign leadership and decisionmakers and cultural factors that may influence decisions. Information is also collected on the nature and characteristics of theater and regional areas of interest. This task also includes collecting against high-payoff targets of national strategic value, whose attack will lead directly or indirectly to the enemys defeat. This collection task requires that deployment transportation information (e.g., threat to and status of transportation infrastructures and ports of debarkation (PODs) en route and within the area of responsibility (AOR)) be collected to support predeployment planning for intertheater and intratheater airlift, sealift, and land movements. This task includes collecting battlefield damage assessments, munitions effects, and medical assessments in order to conduct mission assessment. This task also includes collecting counterintelligence, meteorological, oceanographic, and geospatial (e.g., aeronautical, hydrographic, geodetic, and topographic) information. (JP 2-0 (*JP 3-11, 3-55*))

c. (U) SN 2.3.3 Correlate National Strategic Information. To associate and combine data on a single subject to improve the reliability or credibility of the information. (JP 2-0)

d. (U) SN 2.4.1 Evaluate, Integrate, Analyze, and Interpret Information. To appraise information for credibility, reliability, pertinence, and accuracy (Evaluate). It includes forming patterns through the selection and combination of processed information (Integrate). The task further includes reviewing information to identify significant facts for subsequent interpretation (Analyze). Finally, the task is to judge the significance of information in relation to the current body of knowledge (Interpret). (JP 2-0)

e. (U) SN 2.4.1.1 Identify Global and Regional Issues and Threats. To assess threats to the United States, US military forces, and the countries and forces of our multinational partners. This task includes assessing potential issues and situations that could impact US national security interests and objectives. (JP 2-0)

f. (U) SN 2.4.1.2 Determine Enemys Global Capabilities and Strategic Courses of Action.

To identify, at the national strategic level, what an enemy (or potential enemy) can do, as well as when, and with what strength. This task addresses both military and nonmilitary capabilities. Under military capabilities this task examines ground, air, naval, nuclear, chemical, and biological information warfare; unconventional warfare; and joint capabilities. Nonmilitary capabilities include political and economic actions. This task also includes identifying all strategic courses of action (COAs) open to the enemy and, where sufficient intelligence is available, determining the relative order of probability of each COA. Any factors that may influence the enemy to adopt a COA should be identified. Finally, determination should be made as to the susceptibility of vital elements of the enemys national power to potential actions of another nation. Enemy strategic vulnerabilities may come from political, geospatial (e.g., aeronautical, hydrographic, geodetic, and topographic), climatic, economic, scientific, societal, or military factors. (JP-2-0)

g. (U) SN 2.4.2.1 Provide Worldwide National Strategic Indications and Warning. To report time-sensitive intelligence on foreign developments that could threaten the United States; its citizens abroad; or allied military, political, or economic interests. This task also includes identifying hostile reactions to US reconnaissance activities and indications of impending terrorist attacks. (JP 2-0, 6-0, *(JP 3-5)*)

h. (U) SN 2.4.2.2 Provide Current Intelligence to National Strategic Planners and Decisionmakers. To report strategic intelligence of immediate value relating to particular areas of concern to the National Command Authorities (NCA), strategic planners. This task includes the preparation of intelligence estimates and assessments and periodic intelligence briefings and reports. (JP-20, 6-0)

i. (U) SN 2.5.1 Provide Finished Intelligence Products to National Strategic Planners and Decisionmakers. To provide intelligence information to planners and decisionmakers in a form appropriate to support planning and COA development. (JP 2-0)

j. (U) SN 3.1 Coordinate Forward Presence of Forces in Theaters. To collaborate with other US departments and agencies and the US Congress and to work with foreign governments to allow the stationing of or temporary presence of US combat and support units and individual Service members or DOD civilians. The objective is to allow the rapid application of the military instrument of national security by placing US forces in a position from which they can rapidly respond to a crisis or can support the rapid response of other forces to such a crisis. (JP 3-0, 3-07 *(JP 3-05, 3-07.1, 4-02)*)

k. (U) SN 3.3.4 Apply National Nonlethal Capabilities. To attack in order to affect, modify, neutralize, or destroy strategic-level enemy targets worldwide and in space using nonlethal means. (JP 3-0, 3-12.1, 3-13.1, 3-53 *(JP 3-05.5, 3-11, 3-56.1)*)

l. (U) SN 3.4 Protect Strategic Forces and Means. To safeguard friendly strategic center(s) of gravity, strategic force potential, and bases in the continental United States (includes the civil populace and industrial capacity of the nation) by reducing or avoiding the effects of enemy strategic-level actions and unintentional friendly actions. This task includes protection during strategic deployment of forces. (JP 3-0, 3-01.1, 3-01.5, 3-11 *(JP 3-10, 3-52)*)

m. (U) SN 3.4.5 Coordinate and Conduct Strategic Operations Security. To take actions to minimize friendly indicators associated with national military strategy. This task includes signal security and protection activities (e.g., patterns) strategic forces, and facilities from enemy observation and surveillance (e.g., satellites). (JP 2-0, 3-54, CJCS 3213.01 *(JP 3-0, 3-13.1, 3-55, 3-58, CJCSM 3122.03)*)

n. (U) SN 3.4.6 Protect National Strategic Information, Information-Based Processes, and Information Systems. To defend information, information-based processes, and

information systems by planning and implementing comprehensive defensive information Warfare (IW-D) measures based on a risk-management approach. This task includes ensuring access to timely, accurate, and relevant information when and where needed and to deny an adversary the opportunity to exploit friendly information and systems for their own purposes. (JP 3-0, 3-13.1, 3-54, 3-58 *(JP 1-02, 3-02.1, CJCSI 3210.01)*)

o. (U) SN 4.2.7 Coordinate Defenswide Legal Support. To advise commanders and staffs on all civil, military, international, and operational law issues; to review all rules of engagement (ROE), operation plans, and directives for consistency with US and international law; and to provide legal assistance to military personnel and their families. This task includes overseeing administration of military justice and advice on detention and handling of enemy prisoners of war (EPWs). (JP 3-05.3, 3-57, 5-03.1 *(JP 3-0, 3-10, 3-10.1, 3-15, 3-59)*)

p. (U) SN 5 Provide Strategic Direction and Integration. To develop and revise national and/or multinational military strategy. This task is based on national security strategy for the attainment of strategic security interests, objectives, and end states. The Joint Chiefs of Staff (includes the Chairman and Vice Chairman of the Joint Chiefs of Staff) derive strategic direction from national security strategy and policy directives. The Secretary of Defense, through the Chairman of the Joint Chiefs of Staff, provides strategic guidance and direction to the combatant commanders. The combatant commanders subsequently provide strategic direction for the employment of joint, Service, supporting, special, and multinational forces through their unified action in theater strategies and campaign plans. This task includes providing clear command relationships and tasking authority through an appropriate CJCS planning, warning, alert, or execute order. Theater operations are often in conjunction with interagency, nongovernmental, and private voluntary agencies and UN forces. These three strategies (and related strategic plans) integrate the national ends, ways, and means. (JP 0-2, 3-0, 5-0 *(JP 1-02, 3-07.4, 3-11, 4-01.5, 4-05)*)

q. (U) SN 5.1.1 Communicate Strategic Decisions/ Information. To send and receive strategic decisions and data from one echelon of command, component, Military Department, ally, or other organization to another, by any means. (JP 0-2, 5-0, 6-0)

r. (U) SN 5.1.4 Monitor Worldwide Strategic Situation. To continuously observe and analyze events regionally and globally (including space) in the context of national and multinational security, military strategies, and other elements of national power (i.e., political, economic, and informational). (JP 2-0, 5-0, 6-0, *(JP 3-0)*)

s. (U) SN 5.2.4 Decide on Need for Military Action or Change. To decide whether strategic actions are required which are different from those that combatant command and Service forces have already been directed to support. (JP 1, 0-2, 2-0, 3-0, 5-0)

t. (U) SN 5.3.1 Issue Strategic Planning Guidance. To provide guidance on goals and objectives, resources, and planning tasks to Service staffs, Service major commands, and combatant command planners. This task includes providing guidance for developing recommendations for the national military strategy. It also includes providing guidance for Service forces to ensure they support multinational and theater strategies and campaigns in conformance with DOD, CJCS, and contingency planning guidance. Guidance may include targeting policy, ROE, levels of acceptable risks, and other restrictions and constraints. (JP 1, 0-2, 3-0 5-0 *(JP 2-0)*)

u. (U) SN 5.3.3 Select or Modify Multinational and National Military Strategy, Plans, and Other Strategic Actions. To decide on the strategic option that offers the best prospect for success or to modify a COA previously selected. (JP 1, 0-2, 5-0, *(JP 3-0)*)

v. (U) SN 5.3.4 Review Strategic Options and Recommendations with NCA and Other

Officials and Adjust. To review strategic options and recommended strategies with the NCA and Chairman of the Joint Chiefs of Staff (and Congress and foreign government officials, as required) to enable them to make a reasoned decision. To adjust the recommended strategy or action based on NCA or CJCS guidance. (JP 1, 0-2, 3-0, 5-0, *(JP 2-0)*)

w. (U) SN 5.4.4 Prepare and Issue CJCS Orders. To promulgate national strategic execution decisions to subordinate headquarters as well as directly to executing and supporting forces. This task includes warning, alert, and CJCS execute orders. (JP 5-0, 5-03.1 *(JP 0-2, 3-0)*)

x. (U) SN 5.5 Coordinate Worldwide Information Warfare. To integrate the elements of offensive Information Warfare (IW-O) and IW-D such as physical destruction, military deception, psychological operations, electronic attack, operations security, and other Information Warfare (IW) capabilities in order to affect an adversarys information, information-based processes, and information systems while defending ones own. This task includes military support to attacking and defending IW aspects of national military, political, and economic power. (JP 3-13.1, CJCSI 3210.01 *(JP 2-0, 3-0)*)

y. (U) SN 5.6, Provide Public Affairs (PA) Worldwide. To advise and assist the NCA and Chairman of the Joint Chiefs of Staff, and combined chiefs in a coalition, in telling the militarys story to both internal and external audiences. This task includes originating and assisting civilian news media in preparing both print and broadcast news material and assisting with community relations projects. PA services apply across the range of military operations and are especially applicable in military operations other than war. For example, in a counterinsurgency situation, PA is the function that can influence, educate, and inform the population and still facilitate media operations. (JP 3-07.3 *(JP 1, 0-2, 1-02, 3-0, 3-11)*)

z. (U) SN 8 Foster Multinational and Interagency Relations. To work within the interagency process and with representatives of other nations and regional organizations. This task ensures the accomplishment of US politico-military objectives through the combined action of different US organizations and friends, allies, neutrals, and other nations overseas. (JP 0-2, 3-0, 3-07, 3-13.1 *(JP 3-07.1, 3-07.4, 3-11, CJCSM 3122.03)*)

aa. (U) SN 8.3 Coordinate Military Activities Within the Interagency Process. To work with representatives of the other Executive departments and agencies to resolve issues involving operations both overseas and domestic. This task includes working within the interagency process and establishing informal liaisons to ensure the resolution of differences and the shaping of issues for presentation within the National Security Council System (NSCS). (JP 0-2, 3-0, 3-07, 3-08 *(JP 3-07.1, 3-07.4, 3-57)*)

ab. (U) SN 8.3.2 Conduct Information Management in the Interagency Process. To ensure that the maximum information is made available to all participants in the interagency process. This task includes not only protecting sources of information outside the normal Government information process, it also includes ensuring that the flow of information does not overwhelm the process, thus hiding important facts within a flood of data. (JP 2-0, 3-0, *(JP 3-57)*)

ac. (U) SN 8.3.3 Establish Interagency Cooperation Structures. To work within the interagency process, ensuring knowledgeable personnel represent the views of the Joint Chiefs of Staff and combatant commanders. This task includes the inclusion within the process of those departments and agencies not normally represented in the interagency process, to ensure full coordination within the Executive Branch. This task also includes the establishment, where needed, of informal processes of liaison. (JP 0-2, 3-57)

ad. (U) SN 8.3.4 Perform Consequence Management in the Interagency Arena. To work with the representatives of other Executive departments and agencies to understand the possible paths a developing crisis can take and to provide hedging actions as options for

decisionmakers within the NSCS. (JP 0-2, 3-0)

3. (U) Training Assessment. Table XI-1 depicts a subjective assessment of the joint mission-essential task training accomplished during ER97-1. A comparison is provided with the training assessment from the last two No-Notice Interoperability Exercises, ER95-1 and ER96-1. The assessment is based on the successful or unsuccessful accomplishment of the exercise objectives. Blanks in the table indicate that the UJTL task was not applicable to the specific exercise. It is anticipated that this chart will be updated after future ELIGIBLE RECEIVER exercises in order to track the CJCS JMETL training in this exercise series.

Table XII-1. (U) Training Assessment for ER95-1, ER 96-1, ER97-1

UJTL	ER95-1 ASSESSMENT	ER96-1 ASSESSMENT	ER97-1 ASSESSMENT
SN 2			
SN 2.1.2			
PSN 2.1.3			
PSN 2.1.4			
SN 2.2.1	P		
TSN 2.2.3			
SN 2.3.3	P		
TSN 2.3.4			
PSN 2.4			
SN 2.4.1			
SN 2.4.1.1			
SN 2.4.1.2			
SN 2.4.2.1			
SN 2.4.2.2			
SN 2.5.1			
P			
T			
T			
P			
P			
T			
TSN 3			
SN 3.1			
SN 3.3.4			
SN 3.4			
T			
P			
PSN 3.4.1			
PSN 3.4.2			
SN 3.4.5			
SN 3.4.6	T	P	
P			
PSN 3.5.5			
PSN 3.5.8	P		

~~SECRET~~

Table XII-1. (U) Training Assessment for ER95-1, ER 96-1, ER97-1 (continued)
UJTLER95-1
ASSESSMENTER96-1
ASSESSMENTER97-1
ASSESSMENT
SN 4
SN 4.2.7
SN 5
PSN 5.1.1TTSN 5.1.2PSN 5.1.3
SN 5.1.4P
PT
TSN 5.2.4
SN 5.3.1
PP
T
TSN 5.3.2TPSN 5.3.3
SN 5.3.4
SN 5.3.5
SN 5.4.2
SN 5.4.4
SN 5.5
SN 5.6U
T
P
PP
T

P
T
T
T
P
T
T
PSN 8
SN 8.3
SN 8.3.2
SN 8.3.3
P
P
PSN 8.3.4P

GLOSSARY

AAR	After-Action Review
AF	Air Force
AOL	America On-Line
AOR	Area of Responsibility
ASIM	Automated Security Incident Information Measurement
ASIMS	Air Staff Information Management System
C2	command and control
C3	command, control, and communications
C4	command, control, communications, and computers
C4I	command, control, communications, computers, and intelligence
C	Confidential
CAC	Crisis Action Cell
CAT	Crisis Action Team
CCIR	Commanders Critical Information Requirements
CCWT	Command Center Watch Team
CERT	Computer Emergency Response Team
CIA	Central Intelligence Agency
CINC	commander in chief
CIPWG	Critical Infrastructure Protection Working Group
CIRT	Computer Incident Response Team
CITAC	Computer Investigative and Infrastructure Threat Assessment Center
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff memorandum
CJTF	commander, joint task force
CL BY	classified by
CL REASON	classification reason
CM	Consequence Management
CNA	computer network attack
CNN	Cable News Network
COA	course of action
COMPUSEC	computer security
COMSEC	communications security
CRC	Crisis Response Cell
CSG	Coordinating Sub-Group
CT	counterterrorism
DC	District of Columbia
DCINC	deputy commander in chief
DEFCON	Defense Readiness Condition
DEST	Domestic Emergency Support Team
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIRNSA	Director, National Security Agency
DISA	Defense Information Systems Agency

DLA	Defense Logistics Agency
DMS	Data Management System
DOJ	Department of Justice
DOS	Department of State
EAP	Emergency Action Plan
EEFI	essential elements of friendly information
EEI	essential elements of information
e.g.	for example
EPW	enemy prisoner of war
ER97-I	Exercise ELIGIBLE RECEIVER 97-1
EW	electronic warfare
FAX	facsimile
FBI	Federal Bureau of Investigation
FEST	Foreign Emergency Support Team
FISA	Foreign Intelligence Surveillance Act
FORSCOM	Forces Command
GCCS	Global Command and Control System
GOSC	Global Operations and Security Center
GTS	ground tracking station
HUMINT	human-resource intelligence
IA	information attack
ID	identifier
i.e.	that is
INFOSEC	information security
INMARSAT	International Maritime Satellite
IO	Information Operations
IP	Internet protocol
IPB	Intelligence Preparation of Battlespace
IPC	Information Protection Cell
IPTF	Infrastructure Protection Task Force
IRC	Information Response Cell
ITF	Intelligence Task Force
I&W	indications and warning
IW	Information Warfare
IWG	Intelligence Working Group
JC2WC	Joint Command and Control Warfare Center
JICPAC	Joint Intelligence Center-Pacific
JMET	Joint Mission Essential Task
JMETL	Joint Mission Essential Task List
JWAC	Joint Warfare Analysis Center
LA	Los Angeles
LAN	Local Area Network
LNO	liaison officer
LRC	Logistics Readiness Center
MILNET	Military Network
N/A	not applicable
NBC	nuclear, biological, and chemical

NCA	National Command Authorities
NIEX	No-Notice Interoperability Exercise
NII	National Information Infrastructure
NIPRNET	Non-Secure Internet Protocol Router Network
NMCC	National Military Command Center
NMJIC	National Military Joint Intelligence Center
NNN	NIEX News Network
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSCS	National Security Council System
OATSD(PA)	Office of the Assistant to the Secretary of Defense (Public Affairs)
OCONUS	outside the continental United States
OPLAN	operation plan
OPREP	operational report
OPSEC	operations security
OPT	Operations Planning Team
OSI	Office of Special Investigations
OSR	open source research
P	needs practice
PA	public affairs
PACAF	Pacific Air Forces
PEO	Presidential executive order
POD	port of debarkation
PPP	planning, procedures, and processes
PSYOP	psychological operations
PTER	passive target electronic reconnaissance
RCMP	Royal Canadian Mounted Police
ROE	rules of engagement
S	Secret
SCADA	Supervisory Control and Data Acquisition
SIGINT	signals intelligence
SIPO	Senior Information Protection Officer
SIPRNET	Secret Internet Protocol Router Network
SMG	Secure Mail Guard
SN	Strategic-Level National Military Task
SOF	special operations forces
SOO	Senior Operations Officer
SOP	standing operating procedures
St.	saint
STO	Special Technical Operations
STOC	Special Technical Operations Center
STU	secure telephone unit
T	trained
THREATCON	Threat Condition
TPFDD	Time-Phased Force and Deployment Data
U	Unclassified; untrained

UJTL	Universal Joint Task List
USACOM	US Atlantic Command
USAF	US Air Force
USCG	US Coast Guard
USCINCPAC	Commander in Chief, US Pacific Command
USG	US Government
USPACOM	US Pacific Command
USSOC	US Special Operations Command
USSOCOM	US Special Operations Command
USSPACECOM	US Space Command
USTRANSCOM	US Transportation Command
VAAP	Vulnerability Assessment and Analysis Program
WATCHCON	Watch Condition

(INTENTIONALLY BLANK)

~~SECRET~~

ANNEX A

(U) INDIVIDUAL AGENCY EXERCISE OBJECTIVES

(U) Participant Objectives. Most of the major participants established their own internal exercise objectives. These objectives, by organization, are as follows:

a. (U) Department of State

(b)(1)

[redacted]

b. (U) Federal Bureau of Investigation (FBI)

(b)(1)

[redacted]

c. (U) Defense Intelligence Agency (DIA)

(b)(1)

[redacted]

d. (U) Central Intelligence Agency (CIA)

(b)(1)

[redacted]

e. (U) Defense Information Systems Agency (DISA)

(b)(1)

[redacted]

~~SECRET~~

(b)(1)

f. (U) National Security Agency (NSA)

(b)(1)

g. (U) National Reconnaissance Office (NRO)

(b)(1)

h. (U) US Space Command (USSPACECOM)

(b)(1)

i. (U) US Pacific Command (USPACOM)

(b)(1)

~~SECRET~~

ANNEX B

(U) NIEX EARLY BIRD FOR 11 JUNE 1997

(U) The eight-page Early Bird for 11 June is on the following pages.

(INTENTIONALLY BLANK)