~~SECRET//NOFORN~~

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE

INSPECTOR GENERAL

REPORT OF INVESTIGATION

21 March 2014

IV-13-0051

Alleged Violation of Red Team Standard Operating Procedures

(U) This report might not be releasable under the Freedom of Information Act or other statutes and regulations. Consult the NSA/CSS Inspector General Chief of Staff before releasing or posting all or part of this report.

~~SECRET//NOFORN~~

Approved for Release by NSA on 07-01-2019, FOIA Case # 79204 (litigation)

Release: 2019-06
NSA:08598

(U) OFFICE OF THE INSPECTOR GENERAL

(U) Chartered by the NSA Director and by statute, the Office of the Inspector General conducts audits, investigations, inspections, and special studies. Its mission is to ensure the integrity, efficiency, and effectiveness of NSA operations, provide intelligence oversight, protect against fraud, waste, and mismanagement of resources by the Agency and its affiliates, and ensure that NSA activities comply with the law. The OIG also serves as an ombudsman, assisting NSA/CSS employees, civilian and military.

(U) AUDITS

(U) The audit function provides independent assessments of programs and organizations. Performance audits evaluate the effectiveness and efficiency of entities and programs and their internal controls. Financial audits determine the accuracy of the Agency's financial statements. All audits are conducted in accordance with standards established by the Comptroller General of the United States.

(U) INVESTIGATIONS

(U) The OIG administers a system for receiving complaints (including anonymous tips) about fraud, waste, and mismanagement. Investigations may be undertaken in response to those complaints, at the request of management, as the result of irregularities that surface during inspections and audits, or at the initiative of the Inspector General.

(U) INTELLIGENCE OVERSIGHT

(U) Intelligence oversight is designed to insure that Agency intelligence functions comply with federal law, executive orders, and DoD and NSA policies. The IO mission is grounded in Executive Order 12333, which establishes broad principles under which IC components must accomplish their missions.

(U) FIELD INSPECTIONS

(U) Inspections are organizational reviews that assess the effectiveness and efficiency of Agency components. The Field Inspections Division also partners with Inspectors General of the Service Cryptologic Elements and other IC entities to jointly inspect consolidated cryptologic facilities.

Release: 2019-06
NSA:08599

Doc ID: 6672264

(b) (1)
(b) (3)-P.L. 86-36

I. (U) SUMMARY

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

~~(S//NF)~~ This investigation was conducted in response to a referral from the NSA Office of the General Counsel (OGC). In [redacted] NSA/CSS Information Assurance Directorate (IAD) management officials asked the OGC for legal guidance on certain aspects of authorized IAD Red Team activities conducted in 2011. Those activities were conducted in support of a [redacted] to identify vulnerabilities [redacted] This program is executed with the express knowledge and approval of [redacted] The OGC received allegations by Red Team personnel that information obtained in support of [redacted] concerning [redacted] had not been properly reported.

~~(S//NF)~~ On [redacted], the Red Team reported that [redacted] communications had been successfully accessed due to poor password security. The Red Team was able to read communications between [redacted] and other senior U.S. government officials and gather details of upcoming public activities involving [redacted] and a family member. This information was reported to [redacted]

~~(S//NF)~~ [redacted] During Red Team monitoring of the DoD Non-classified Internet Protocol Router Network system (NIPRNet) [redacted] operators observed what they believed to be evidence of an adulterous relationship between [redacted] and [redacted] The Red Team also observed what analysts believed may be classified information transmitted by [redacted] concerning [redacted] Red Team analysts orally reported to the Red Team chain of command a possible violation of the Uniform Code of Military Justice (adultery) and their concerns regarding the unauthorized disclosure of classified information. This information was not reported to anyone outside the Red Team.

~~(S//NF)~~ [redacted]

~~(S//NF)~~ On 20 July 2011, Red Team analysts submitted a final report on [redacted] computer activity to Red Team management. This report contained analytic conclusions about [redacted] relationship with [redacted] and the potentially classified [redacted] details discovered on [redacted] unclassified government computer. This information was not properly reported under the Red Team's Standard Operating Procedures.

~~(S//NF)~~ As a result of our inquiry, we conclude that [redacted] failed to ensure that the Red Team took required actions to report incidents when they discovered potentially classified material on [redacted] unclassified machine and when they received allegations of a possible violation of Article 134 (adultery) of the Uniform Code of

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

Release: 2019-06
NSA:08600

(b) (1)
(b) (3)-P.L. 86-36

Military Justice by [redacted] in violation of NSA IAD I741 *Red Team SOP Incident Response and Activity Documentation,* 14 June 2010.

(U//~~FOUO~~) A copy of this Office of the Inspector General report will be forwarded to the NSA/CSS Associate Directorate for Security and Counter Intelligence, the NSA/CSS Office of Employee Relations, the Department of Defense Inspector General, and the [redacted] for information and action deemed appropriate.

(b) (6)

Release: 2019-06
NSA:08601

II. (U) BACKGROUND

(b) (1)
(b) (3)-P.L. 86-36

(U) Introduction

(S//NF) NSA Red Team assessments of computer networks began in The assessments were conducted under various operational names sponsored each operation.

(U//FOUO) The Red Team for included operators, analysts, and a civilian team leader. The operators were mainly junior grade enlisted military personnel. The analysts and team leader were NSA civilians. The team reported to an operations manager a deputy division chief and a division chief The division chief reported directly to reported to the chief, a NSA senior,

(b) (3)-P.L. 86-36

(S//NF) the Red Team first exploited the government computers used by the Red Team notified that the computers had been exploited due to poor password security. the Red Team observed and a woman later identified as that indicated to the operators and analysts that may have been committing adultery, a possible violation of Article 134 of the Uniform Code of Military Justice. The Red Team also detected in email sent potentially classified information regarding This information was orally reported to the Red Team deputy division chief and division chief. The Red Team division chief orally passed this information to The analysts and team leader were then tasked with writing a report of their findings. This report was provided to the Red Team division chief on 20 July 2011. passed this information to

(S//NF)

(U//FOUO) After an OGC meeting with Red Team personnel in OGC referred this matter to the OIG.

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

Release: 2019-06
NSA:08602

(U) Applicable Authorities

(U) These authorities were reviewed during this investigation. See Appendix A for the full citations.

- NSA/CSS Policy 5-5, Reporting Of Security Incidents and Criminal Violations
- Title 10, U.S. Code §934 (Uniform Code of Military Justice, Article 134)
- Directive-Type Memorandum (DTM) 08-052 DoD Guidance for reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters
- NTISSD No. 600, Communications Security (COMSEC) Monitoring
- NSA IAD [redacted] Red Team SOP, Incident Response and Activity Documentation

(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08603

III. (U) FINDINGS

(U//~~FOUO~~) Issue: Did [redacted] fail to report information to appropriate authorities possible violations of federal criminal law, as NSA/CSS Policy 5-5, Reporting of Security Incidents and Criminal Violations requires?

***(U//~~FOUO~~) CONCLUSION:* Unsubstantiated.**

(U//~~FOUO~~) Issue: Did [redacted] fail to report information related to a significant crime to a military commander or law enforcement agency with appropriate jurisdiction as NTISSD No. 600 requires?

(U//~~FOUO~~) CONCLUSION: Unsubstantiated.

(U//~~FOUO~~) Issue: Did [redacted] fail to ensure that the Red Team took required actions to report and respond to incidents as required by Red Team SOP?

(~~S//NF~~) CONCLUSION: Substantiated. *The preponderance of the evidence supports the conclusion that [redacted] failed to ensure that the Red Team took appropriate actions to report and respond to information that [redacted] may have been involved in criminal activity by engaging in adultery in violation of UCMJ article 134 and that he inappropriately passed potentially classified information through an unclassified computer network.*

(U//~~FOUO~~) Issue: Did [redacted] fail to report information or ensure that the information was reported to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), as DTM 08-052 requires?

(U//~~FOUO~~) CONCLUSION: Unsubstantiated.

(b)(3)-P.L. 86-36
(b)(6)

(b)(1)
(b)(3)-P.L. 86-36

(U) Documentary Evidence

~~(S//NF)~~ [redacted] **email,** [redacted] emailed Agency management to notify them that the Red Team had successfully exploited the NIPRNet computers used by [redacted] also reported that he had notified external customers of the exploitation. This email contained an attachment which provided a timeline of that exploitation, examples of exploited information, such as communications with senior government officials and [redacted] and mitigation recommendations. This email was classified as SECRET//NOFORN (Appendix B).

~~(S//NF)~~ **Red Team Analyst Report,** [redacted] This report contains a synopsis of data obtained from [redacted] NIPRNet account by the NSA Red Team. This report summarizes the information obtained by the Red Team regarding the potential for foreign intelligence service

(b)(3)-P.L. 86-36

(b)(6)

Release: 2019-06
NSA:08604

(b)(1)
(b)(3)-P.L. 86-36

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

IV-13-0051

exploitation of [redacted] and [redacted] due to her "close relationship" with [redacted] and details regarding [redacted] that [redacted] sent on the unclassified network. The Red Team [redacted] The Red Team also identified an unclassified email domain [redacted] Email in this domain was used to transmit information about [redacted] This report was sent to [redacted] Red Team, and [redacted] Red Team (Appendix C).

(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Agency Computer Records.** The OIG conducted a review of computer records and accounts associated with [redacted] and [redacted] This review confirmed that the Red Team analyst report dated 20 July 2011 was sent to [redacted] Red Team, and [redacted] Red Team, on 20 July 2011. The review was unable to verify that the Red Team analyst report cited above was sent electronically to [redacted]

(S//~~NF~~) **Red Team Zip File.** Witnesses interviewed testified that a zip file containing screen shots from [redacted] NIPRNet accounts obtained by the Red Team was created and password protected. Testimony indicated that the password [redacted] office. The OIG searched the [redacted] office and found [redacted]

(S//~~NF~~) [redacted] The program objectives include identifying and exploiting potential vulnerabilities [redacted]

(b)(3)-P.L. 86-36
(b)(6)

Surveillance and other operations may be conducted against [redacted] (Appendix D).

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Red Team SOP, Incident Response and Activity Documentation (14 June 2010).** The SOP describes documentation requirements for normal NSA Red Team operations and identifies steps for reporting incidents outside normal activities. The SOP includes the detection of possible criminal activity and misuse of Government information systems as a significant reportable activities (Appendix E).

Release: 2019-06
NSA:08605

(b) (1)
(b) (3)-P.L. 86-36

~~SECRET//NOFORN~~

IV-13-0051

~~(S)~~ **Red Team Supplemental Rules of Engagement and Objectives for** The Rules of Engagement state:

~~(S//NF)~~ NSA Red Team objective (f) states:

~~(S//NF)~~ **Classification Review of Red Team Analyst Report, 20 July 2011.** On 5 April 2013 provided a classification review of the Red Team Analyst Report. consulted with AD classification authorities and determined that the information pertaining to is classified SECRET//NOFORN. (Appendix G).

(U) Testimonial Evidence

(b) (6)

(b) (3)-P.L. 86-36

(U//~~FOUO~~) ***Management for Operation***

(U//~~FOUO~~) On 24 April 2013 managers of the provided insight on to the OIG. Red Team members present during the meeting were DoD Red Team, DoD Red Team, and DoD Red Team. management provided the following information pertaining to rules of engagement.

~~(S//NF)~~ did not restrict Red Team access to its computers. All computers were subject to Red Team monitoring during

~~(S//NF)~~ Under expected the NSA Red Team to conduct a two-fold mission: assess network vulnerabilities and search for information of interest to foreign intelligence services that could lead to personnel vulnerabilities.

~~(S//NF)~~ expected the NSA Red Team to report questions that pertained to the was not interested in receiving reports on matters outside the mission. If the NSA Red Team monitoring discovered reportable information outside the scope of expected that the NSA Red Team would follow NSA reporting procedures.

(U//~~FOUO~~) ***Red Team Operator***

(U//~~FOUO~~) was interviewed on 19 December 2012 and provided the following sworn testimony.

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08606

(b) (1)
(b) (3)-P.L. 86-36

~~SECRET//NOFORN~~

IV-13-0051

~~(S//NF)~~ In [redacted] while working for the Red Team, [redacted] became aware of [redacted] Initially Red Team personnel [redacted] It was eventually determined that [redacted]

~~(S//NF)~~ [redacted] Red Team members were concerned about [redacted] extramarital affair. (b) (3)-P.L. 86-36

~~(S//NF)~~ The information was initially reported to Red Team [redacted] who said that he would report the concerns to the next level of management. [redacted] Sometime after the initial report, [redacted] and other team members attended a meeting with [redacted] and [redacted] deputy, to discuss Red Team concerns about [redacted] communications. [redacted] told the team that the information pertaining to [redacted] would be reported up the management chain. Ultimately, someone in Red Team management decided not to view any more of [redacted] emails. [redacted] heard second hand that the information was reported to [redacted] but not reported further. [redacted] believed "this was a bad decision. [redacted]

(U//~~FOUO~~) [redacted]
Red Team Operator)

(U//~~FOUO~~) [redacted] was assigned to the Red Team [redacted] was interviewed on 8 January 2013 and provided the following sworn testimony. (b) (6)

~~(S//NF)~~ [redacted] was the Red Team operator who directly monitored [redacted] computer activity as part of [redacted] He viewed [redacted]

~~(S//NF)~~ At first, [redacted] thought that these emails were not something the Red Team should be reviewing. He changed his mind once there was a discussion within the Red Team about the counterintelligence concerns the emails created. He agreed with the other team members that the emails [redacted] presented a counterintelligence concern and that the team would be acting appropriately by reporting this information to Red Team management. A report was eventually prepared by the [redacted] and the team's [redacted] did not see the report and does not know

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08607

who the report was sent to. The team was "going by the book" in reporting their counterintelligence concerns about to management.

(S//NF) Someone on the team created two zip files which contained and created a random password to protect these files. He used as many as twenty random characters for the password. He was unable to recall the password. He inside a navy blue, two pocket folder. He then stored the folder in a 4 or 5 drawer safe within Red Team work space. He does not know if the folder containing this password is still within Red Team space.

(S//NF) had left and the Red Team when the information about

(U//FOUO) ***Red Team Operator***

(b)(1) (b)(3)-P.L. 86-36

(U//FOUO) was interviewed on 19 December 2012 and 10 April 2013. He provided the following sworn testimony.

(S//NF) was part of the Red Team when it was monitoring personnel, including The monitoring was part of The Red Team did not target

recalled viewing communications could not recall. that only contained email

(b)(6)

(S//NF) This information was reported to who then reported it to the Later, the entire team was called into office for a meeting. deputy also attended the meeting. During the meeting, the team was instructed to stop all operations associated with and not to speak of the traffic the team had found to anyone outside the Red Team. He recalled telling the team operators that "they did not know what they saw" in regard to Management believed that there was not enough evidence of wrongdoing to report it. did not agree with the decision not to pursue this matter because he thought the information made He believed that should have been made aware of the information.

(S//NF) heard no more about the information until the team was requested to perform a data scrub to remove all "personal" information from the systems. The request to remove data pertaining to came before the fact that was having an affair told a team operator, to delete information pertaining to from the Red Team records. is not certain

who in the management chain was consulted before this decision was made but believes that [redacted] made the decision. A password protected encrypted file was created containing the correspondence from [redacted] No one has been able to recall the password.

(b)(1) (b)(3)-P.L. 86-36

(U//~~FOUO~~) [redacted] ***former Red Team Operator***

(U//~~FOUO~~) [redacted] was telephonically interviewed on 16 April 2013. He had deployed to an overseas location. [redacted] provided the following information.

(~~S//NF~~) [redacted] was a member of the [redacted] Red Team while [redacted] While [redacted] was a Red Team operator, [redacted] directed him to delete all information the team had collected pertaining to [redacted]

(U//~~FOUO~~) [redacted] ***Chief,*** [redacted] (b)(3)-P.L. 86-36 (b)(6)

(U//~~FOUO~~) [redacted] was interviewed on 20 December 2012 and 10 April 2013. He provided the following sworn testimony.

(U//~~FOUO~~) [redacted] was a member of the Red Team [redacted] He was [redacted] until his departure.

(~~S//NF~~) [redacted] was a [redacted] sponsored exercise to identify vulnerabilities that an adversary could use to access classified or sensitive information. The team attempted to look for data that an adversary could use to target leadership. "We would look for anything a real adversary would look for."

(b)(3)-P.L. 86-36

(~~S//NF~~) OIG personnel told [redacted] the OIG had been told that the Red Team had strayed from conducting network analysis and was conducting an unauthorized investigation of [redacted] objected to that assertion. [redacted] said that [redacted] differed from a typical Red Team operation. Normally, the Red Team would only be asked to look for network vulnerabilities. However, with [redacted] the team was also asked to conduct a full spectrum vulnerability assessment that consisted of looking at vulnerabilities to networks and personnel. The team was authorized to look on [redacted] computer networks for information useful to hostile agents. The team would not have been able to fulfill the full spectrum analysis had they not been able to target computers of [redacted]

(~~S//NF~~) [redacted] He was considered a legitimate target of [redacted] the team gained access to the government computers used by [redacted] was notified and told the team to continue to monitor [redacted] computers. The team [redacted] the computers [redacted] used and occasionally took screen shots of his computers. His systems were monitored until [redacted]

(b)(1) (b)(3)-50 USC 3024(i) (b)(3)-P.L. 86-36

(b)(1) (b)(3)-P.L. 86-36

Release: 2019-06
NSA:08609

(S//NF) The Red Team did not target [redacted] They did not attempt to [redacted]

(S//NF) In late [redacted] asked a team operator if anything new was happening with [redacted] The operator immediately did a screen capture and they saw an [redacted]

(S//NF) The Red Team is made up mainly of enlisted military personnel [redacted] was having an affair with [redacted] was "really bad." Collectively, the team thought this information should be reported up the chain for a decision on what to do. [redacted] the Red Team [redacted] was notified, and he also agreed that it was "bad." [redacted] does not know if [redacted] informed his immediate supervisor, [redacted] However, the next day [redacted] came into the team's work area and said: "You guys aren't in trouble. You aren't breaking the law. You don't know what you saw."

(b)(6)

(b)(3)-P.L. 86-36
(b)(6)

(S//NF) [redacted] did not agree with [redacted] because "we all knew what we saw." There was no doubt in his mind that [redacted] was having an affair with [redacted] One of the things that [redacted]

(S//NF) [redacted] thought that [redacted] He thought this was a foreign intelligence risk. [redacted] thought that the relationship between [redacted] posed a counterintelligence risk [redacted]

(S//NF) [redacted] printed screen shots of what the Red Team operators had captured after he realized the implications of what they contained, information that [redacted] was having an affair with [redacted] showed them directly to [redacted] and [redacted]

(S//NF) [redacted] told [redacted] and [redacted] daily that the Red Team had seen emails from [redacted] on the unclassified network that contained classified information about [redacted] He repeatedly recommended that management report the information the team had found regarding [redacted] relationship with [redacted] because he thought there was a counterintelligence concern. He spoke to [redacted] and [redacted] daily about his concerns and also discussed them at weekly operations meetings that [redacted] attended.

(S//NF) [redacted] believed that the counterintelligence vulnerabilities pertaining to [redacted] should have been reported to the appropriate government officials. [redacted] continued daily to implore management to elevate this matter. It was brought up in meetings

Release: 2019-06
NSA:08610

Doc ID: 6672264
(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-50 USC 3024(i)
(b) (3)-P.L. 86-36

regularly, specifically the belief that [redacted] should be investigated. [redacted] believed that management continued to focus on the affair itself rather than the counterintelligence concerns associated with the relationship.

~~(S//NF)~~ [redacted] relationship with [redacted] and [redacted] deteriorated as a result of his continually telling them that the information concerning [redacted] should be reported. He eventually applied for and was selected for a position with another organization within NSA. Once his pending move became known to his management, he was reassigned to an empty office for 60 days without being given any work. [redacted] thinks he was given a lower performance evaluation because of this incident but has no evidence to support this belief.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) [redacted] ***Senior Analyst,*** [redacted]

(U//~~FOUO~~) [redacted] was the [redacted] for the Red Team [redacted] was interviewed on 28 March 2013 and provided the following sworn testimony.

(b) (6)

~~(S//NF)~~ The Red Team received permission [redacted] government computers. The initial request went from [redacted] to the [redacted] and then to [redacted] The approval came back from [redacted] through the [redacted] to [redacted] who orally informed the Red Team that the request had been approved.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//NF)~~ It was typical for the Red Team to review emails on targeted systems and computers of [redacted] and [redacted] knew that the team was looking at [redacted]

~~(S//NF)~~ Initially the emails between [redacted] were professional and were about [redacted] Eventually the team started seeing emails about [redacted] At some point the [redacted] saw numerous [redacted]

~~(S//NF)~~ The team also collected emails [redacted] The emails also contained information about [redacted] thought that the emails were at least classified CONFIDENTIAL.

~~(S//NF)~~ [redacted] and another team analyst, [redacted] prepared a report citing their counterintelligence concerns regarding [redacted] The report was provided to [redacted] and [redacted] believed that [redacted] and [redacted] wanted to "keep this matter quiet and not reported." [redacted] and [redacted] were both hands-off managers who were "being inconvenienced by this report." He remembered asking [redacted] and [redacted] at least six times about sending the report forward. [redacted] gave [redacted] and [redacted] the opportunity to look at the emails the operators had seen, but [redacted] is not sure if they ever actually looked

(b) (3)-P.L. 86-36
(b) (6)

(b) (3)-P.L. 86-36

Release: 2019-06
NSA:08611

at them told the operators that what they saw "was not a big deal" and that the operators had misconstrued what they had seen.

~~(S//NF)~~ It was opinion that it was impossible to get and engaged in team operations and that the information found by the team regarding was "inconvenient" for them. were given poor performance evaluations because of their reporting on this matter, and told that he would not be promoted because of his persistence in recommending that this matter be reported to IAD management and

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

(U//~~FOUO~~) ~~Team Leader~~

(U//~~FOUO~~) was assigned to the Red Team as an analyst and technical leader from He was interviewed on 28 March 2013 and provided the following sworn testimony.

~~(S//NF)~~ was an exercise in which through asked the team to assess vulnerabilities to systems and personnel. The team and The customer, in this case told the team which computer addresses they could not target. The team, through informed and that they had access to the computer used. There was no instruction from or for the team to stop monitoring his computer. The monitoring of computer was an authorized activity under

(b) (6)

~~(S//NF)~~ Initial screen shots capturing Later screen shots revealed that the communications were He heard that had shown these screen shots to and

~~(S//NF)~~ The team had concerns that was in violation of the Uniform Code of Military Justice The team also captured screen shots indicating that was passing classified information The team had counterintelligence concerns because and they thought that the information should be forwarded to

(b) (3)-P.L. 86-36

~~(S//NF)~~ told team operators and analysts that they did not know what they had seen regarding and that they should leave this issue alone and forget about what they had seen.

~~(S//NF)~~ The team put all of the information pertaining to in a zip file and protected the file with a password.

~~(S//NF)~~ The decision to not notify the IAD Office of General Counsel of information found by the team was made by and The information collected on

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36

Release: 2019-06
NSA:08612

was reportable, but did not want to go outside the chain of command because and thought that he would be fired.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) *Chief,*

(b)(6)

(U//~~FOUO~~) was interviewed on 16 April 2013 and provided the following sworn testimony.

(U//~~FOUO~~) was the chief of operations for the Red Team from He supervised technical and team leaders assigned to the Red Team operations, including

(~~S//NF~~) The true impact of the Red Team is to report to senior leaders what information the team is able to exploit, not in "simply telling them they have a problem with a computer router."

(b)(1)
(b)(3)-P.L. 86-36

(~~S//NF~~) was unique in that this operation allowed the team to look for

(~~S//NF~~) and reported several problems associated with that made him vulnerable to a foreign intelligence service. made the decision not to report this information outside NSA.

(~~S//NF~~) discussed the need to report the counterintelligence vulnerabilities described in the analyst report associated with with and and was told that "they would handle it." He had another discussion with on this matter and was told Red Team leadership did not want to report the information and "it was time to move on." The information should have been reported in a Significant Activity Report.

(~~S//NF~~) and said that ordered them to "get rid of the files" the team had collected on The normal process for deleting information is to wait until an after-action report had been completed and provided to the customer. did not agree with the decision to delete this information. He believes that the team did not comply with the rules of engagement by not reporting the information about and by having the information deleted.

(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~)

(U//~~FOUO~~) was interviewed on 15 May 2013 and provided the following sworn testimony.

(U//~~FOUO~~) was the Deputy Chief, Red Team, from He reported directly to He was the of approximately subordinate military members assigned to Red Team operations. He spent most of his time writing awards and assessments for subordinates while assigned to this position. He also assisted in providing strategic direction for Red Team activities.

(b)(3)-P.L. 86-36

(b)(6)

Release: 2019-06
NSA:08613

(U//~~FOUO~~) does not recall written guidelines describing what information was required in a Significant Activity Report (SAR). Typically, Red Team leaders would orally present information to him and and they would decide to issue a SAR or present the information to their manager for a decision on whether to report a concern. Usually he was not present when presented information to

(S//~~NF~~) was told by and that the Red Team had discovered information indicating that was having an affair. He never asked to see the information the team had collected. told him that he was going to report this information to

(U//~~FOUO~~) saw the analyst report, dated 20 July 2011 and had prepared. He discussed this report about a half dozen times with and they decided to notify presented this information to did not witness informing about the information in the analyst report, but told him that he was going to pass the information to and has no reason to doubt that he did.

(U//~~FOUO~~) believes that sent the analyst report to They expected that the analyst report would be routed appropriately and handled with sensitivity. As far as he and were concerned, they reported the information up the chain to and did not let sensitive information "rest with them."

(b)(3)-P.L. 86-36
(b)(6)

(U//~~FOUO~~) ***former Division Chief, Red Team***

(U//~~FOUO~~) was interviewed on 8 July 2013 after returning from an overseas deployment. provided the following sworn testimony.

(U//~~FOUO~~) was the Division Chief for the Red Team from He reported directly to

(b)(6)

(U//~~FOUO~~) The challenge for Red Team is to present vulnerability information to customers to show the importance of protecting their networks. The Red Team is not relevant if customers do not act upon information provided to them. Red Team operations are always about the information vulnerability, not just network vulnerabilities. Each Red Team spends a lot of time looking for "that nugget of information" to make someone understand why network security is important.

(b)(3)-P.L. 86-36

(S//~~NF~~) There were daily, morning meetings with regarding The team had gained access to the government computers used. There was no question that the team was authorized to access those computers.

(S//~~NF~~) In approximately reported to that the team had collected email communications between and about The team also determined that had not changed his password in years reported this information to and believes that this information was passed to external customers.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ In the timeframe told that the team had captured screenshots from government computer indicating was having an affair with Team members tried to show screen shots of communications with but he did not want to see them. He orally reported this information to who was not happy hearing that the team had found this information and asked him if the team was doing what they were supposed to be doing said he was going to "talk to the guys in the war room about what they had found." viewed intention to speak directly to the team operators as unusual. He told his deputy to make sure that one or both of them were in the room when spoke to the operators. "went off on his own" and spoke to the team operators directly without or being there and told that came into the war room and told them and the rest of the team that they needed to forget what they had seen about the alleged affair between and not talk about it to anyone.

(b)(3)-P.L. 86-36

~~(S//NF)~~ In the time frame came to him and reported that the team had seen details about He told to prepare a report about the information. He specifically instructed to leave out any reference to the alleged affair. He knew that he would be providing this report to who would then be providing it to the customer. However, when he received the report from it contained a paragraph about the affair between He deleted the paragraph and sent the report, via email, to

~~(S//NF)~~ did not want to include the paragraph on the alleged affair because he wanted the report to have a broad distribution so the customer could fix the network vulnerability. also thought the analysts were wrong in their conclusions about having an affair with recalled that the analyst team involved in this issue had made a wrong conclusion about a previous, different issue and thought that this was another example where they had reached the wrong conclusion.

~~(S//NF)~~ told that he had tasked the analysts with writing a report on the information found on government computer. asked him numerous times if the analyst report was finished and reminded him numerous times to make sure he was sent the report. believes that he sent the analyst report to more than once and knows that he sent parts of it to as he was receiving them. He kept involved in all aspects of the team's monitoring of government computers because he was new to the job.

(b)(3)-P.L. 86-36

~~(S//NF)~~ had many discussions with about what the team had found regarding However, he did not know what happened to the information. He recalled having a conversation with when the information surfaced. The conversation was in office, and the two discussed whether to provide the information to someone They talked about whether there was a way to tell an that "they have a potential network issue." The team did not have a customer relationship and he and were trying to be careful with how they reported this information. The information met a threshold to do something other than the standard reporting described in

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08615

the SOP. He recognized that there was "something different here" and he needed to report this information to his management due to its sensitivity and association with

(U//~~FOUO~~) recalled sending the analyst report to and discussing it with him. If says he doesn't know anything about the information in the analyst report that means that he forgot, because he was told." remembers initially discussing the analyst report with and then coming back to discuss it again a few weeks later. He never received any information from as to what he did with the analyst report. At the time he did not know what information communicated up the chain of command or if he passed the analyst report to anyone else.

(~~S//NF~~) thinks that a possible reason for not providing the analyst report to anyone was that and the information contained in the analyst report had "been overcome by events." The vulnerabilities noted in the analyst report may have been viewed as no longer relevant because stopped "pushing" the issue with once He believed the information the team collected on was reportable because it demonstrated the potential impact of poor network security.

(b) (3)-P.L. 86-36

(~~S//NF~~) recalled being concerned that the information captured by the team contained personally identifiable information (PII) pertaining to Information is considered PII if it is information that is personal in nature and is not related to the mission and function of the customer. In view, this definition of PII "is probably broader than the official definition of PII." An example of information meeting his definition of PII is someone sending an email on a government computer about "wanting to buy a boat." While this email did not include personal identifying information, such as a social security number or date of birth, it dealt with a "personal event" and therefore met his definition of PII.

(~~S//NF~~) There was a general practice within the Red Team to keep information that had been collected for long periods of time. There was no clear policy to address what information should be retained or how long. In approximately management started to develop procedures for data collection, retention and storage. thought that the team was keeping data for long periods of time for no good reason. During management discussions about data storage and retention, he went to a member of the team and told him to delete the information pertaining to knew that was no longer in and was, therefore, no longer a target of the operation. He also instructed to make sure that they had uninstalled monitoring devices from the government computer used. He told that the team could retarget that particular computer once He said the deletion of information within the team was not just about deleting information pertaining to management was trying to enact standards across the board to address data retention practices.

(b) (1)
(b) (3)-P.L. 86-36

Doc ID: 6672264

(U//~~FOUO~~) Regarding reporting requirements, Operators received formal training, and Standard Operating Procedures (SOPs) covered the basics of what to do; when to do it, and what to report. The Red Team SOPs applied to all operations "across the board."

(S//NF) At any time there were Red Team operations ongoing, had a good grasp of the generalities of but was not familiar with the details of that operation. The operation was a little different because the customer was even though the operation involved monitoring networks. Additionally, was unlike other operations because He spent more time on the other Red Team operations because of and his responsibility to issue after action reports.

(U//~~FOUO~~)

(U//~~FOUO~~) was interviewed on 20 December 2012, 10 May 2013, and 13 September 2013. He provided the following sworn testimony.

(b)(3)-P.L. 86-36
(b)(6)

(U) **20 December 2012 interview**

(b)(3)-P.L. 86-36

(S//NF) when the Red Team began to monitor the email traffic of The first vulnerability discovered related to was in when the Red Team noticed that was sending on an unclassified network official traffic of a sensitive nature and that This information was reported to external customers.

(S//NF) In early group chief, told him that there was speculation from Red Team operators that "there was an affair going on involving " He did not personally view emails and communications attributed to nor did he get specifics about their contents. He was told that "may have been having an affair," reason for bringing this issue to his attention was to determine what should be done with the information.

(S//NF) believed that the Red Team should not pursue "things of a personal nature" and provided this instruction to "It seemed outside of the bounds of what the Red Team's charter was in handling personal type information." He spoke with the Red Team operators inside the operations room and asked them, at the time, if they were sure this information was coming directly from The operators could "not give me a definite 'yes'." He also asked the operators if someone else could have had access to computer and was told that "yes, someone else could have had access."

(U//~~FOUO~~) decided not to have this information pursued further. He did discuss his decision with his supervisor, who agreed with him. He did not consult with anyone at a higher level within NSA about this matter.

(S//NF) believed there was no definitive evidence of a crime and the Red Team was not involved in counterintelligence; so that avenue was not pursued. Aides to also could have had access to his email accounts. He performed all necessary due diligence

Release: 2019-06
NSA:08617

before making his decision and, in hindsight, would come to the same conclusion, in spite of the

~~(S//NF)~~ If the speculation of the Red Team operators was correct, there would have been other people closer to who would have been aware of the affair. If we had absolute evidence of an affair I guess I would have considered it. "That article of the UCMJ is hard to prove and often not pursued. That also factored into my decision."

(U) ***10 May 2013 interview***

(U//~~FOUO~~) was represented by during this interview. was given a rights warning before the interview and was told that he was suspected of having failed to comply with Directive Type Memo (DTM) 08-052 *Questionable Intelligence Activities and Significant or Highly Sensitive Matters* and NSA Policy 5-5, *Reporting of Security Incidents and Criminal Violations*. provided the following voluntary, sworn testimony.

(U//~~FOUO~~) The first time he read the DTM-08-052 and NSA Policy 5-5 was on 6 May 2013 after receiving these documents from the OIG. He was unaware of the reporting requirements under this Directive and Policy. He was never informed by the NSA OGC that the reporting requirements specified in these documents applied to the Red Team.

~~(S//NF)~~ The Red Team had the approval of and to monitor the government computers used.

~~(S//NF)~~ The passing of classified information on an unclassified computer would be something the Red Team would report. was not told or shown any information that had passed classified information over the unclassified government computer network. The first time he saw the Red Team analyst report was in

~~(S//NF)~~ was not given details about what the Red Team operators found regarding affair with or both, gave him an oral report that the operators had found information that made them suspicious that may be having an affair. He did not ask to see the information that the operators had seen and did not ask or to provide information to him. He had trust in his subordinate leaders that they would have provided an accurate representation to him as to what the operators had seen. It would have been inappropriate for him to look at the information because he was two to three levels removed from Red Team operations.

~~(S//NF)~~ claimed that he did not order the deletion of any information collected by the Red Team pertaining to

(U) ***13 September 2013 interview***

(U//~~FOUO~~) This interview was conducted to give an opportunity to address differences between his testimony and testimony provided by his subordinate,

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

(b) (6)

(b) (1)
(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36

(b) (3)-P.L. 86-36
(b) (6)

(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

Release: 2019-06
NSA:08618

Doc ID: 6672264

was advised of his rights and consented to a voluntary interview without legal representation. provided the following sworn testimony.

~~(S//NF)~~ did not recall talking with about contacting regarding the information the Red Team exploited from computers. He did recall discussing information seen by the Red Team that but the main thrust of this discussion was the alleged affair was having with This discussion was either with or one of the Red Team analysts. This discussion probably took place before or in early not too much longer after this discussion.

(U//~~FOUO~~) did not see the Red Team analyst report from 20 July 2011 until There is a possibility sent this report to him via email in July 2011, but he did not receive it or failed to read it.

~~(S//NF)~~ Any members of the Red Team could have discussed their concerns about with NSA lawyers or other NSA managers without going through the Red Team chain of command. Red Team members did not have to rely upon his approval to along their concerns.

(b)(3)-P.L. 86-36

~~(S//NF)~~ In opinion, the information provided to him about amounted to nothing beyond analytical speculation. He did not see any of the raw data the analysts had seen and was not presented with any evidence that met the criteria for reporting.

(U//~~FOUO~~) ***Chief,***

(b)(3)-P.L. 86-36

(b)(6)

(U//~~FOUO~~) DISES, was interviewed on 31 January 2013 and provided the following sworn testimony.

~~(S//NF)~~ has been the chief of since He had been the chief of for when and orally informed him that Red Team operators found indications that may have been having an affair with He did not see the analyst report pertaining to or know of this reports existence, until made no mention to him of any counterintelligence concerns associated with when informing him of this matter in July 2011.

~~(S//NF)~~ In July 2011, and told him that the team had seen vague information indicating that "may have an issue with " He understood this to mean that the team was making an accusation that there could be an affair but did not have specific information to support this claim. He agreed with the assessment made by and that this was not a reportable incident. He suggested to that he should meet with team operators to get more information as to what they saw. reported back to him that team operators said they had not seen any evidence of a reportable crime and they could not be 100% sure that the communications they saw actually came from and not someone else using computer.

Release: 2019-06
NSA:08619

~~(S//NF)~~ made the decision to stop the team's monitoring of computer, and supported that decision. He had a strong sense at the time that the team was out of bounds and that they needed to "get off of computer." The decision to stop monitoring computer was made on the day he heard about the alleged affair or within a day or two later.

~~(S//NF)~~ In the Red Team reported a problem involving His failure to change his computer password believed this was an appropriate example of the Red Team reporting a vulnerability.

(b)(3)-P.L. 86-36

~~(S//NF)~~ Sometime between the team operation changed from one of assessment to His first concern as the new chief of was that team operators

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ In opinion, the Uniform Code of Military Justice (UCMJ) is not applicable to Red Team operations. "Anyone who thinks the UCMJ applies to what the Red Team does is showing their ignorance about the Red Team mission." The team has an obligation to report significant crime to the NSA Office of General Counsel and "possible violations of the UCMJ are never considered." "Rule number one of Red Team operations is that the team should avoid files containing personal information

(U//~~FOUO~~) stated "NSA/CSS Policy 5-5 is a global, over-arching high level and vague document focused on reporting criminal violations." While having respect for Policy 5-5, referencing this document in this scenario "is a stretch because IAD has specific policy documents which guide Red Team operations."

(b)(3)-P.L. 86-36

(U//~~FOUO~~) According to "NSA does not have a counterintelligence mission and IAD does not have a counterintelligence mission." The Red Team was reporting information that was clearly of "a personal nature and out of bounds." A Significant Activity Report should not have been generated by the team and, had that report been disseminated, IAD would have been in "violation of DoD and IAD policy." The right decision was made to not disseminate the analyst report.

(U//~~FOUO~~) ***Owner, Chief Executive Officer,***

(U//~~FOUO~~) was interviewed on 14 June 2013 and provided the following sworn testimony. Before his interview with the OIG, was re-indoctrinated for access to TOP SECRET//Special Compartmented Information by the ADS & CI.

(U//~~FOUO~~) was the acting chief of from He was the Deputy Chief, His duties included managing Red Team and Joint COMSEC Monitoring Activities. He resigned from Agency employment

(b)(6)

Release: 2019-06
NSA:08620

~~(S//NF)~~ management duties included maintaining oversight of Red Team activities. told him about the team's access to government computers and expressed concern about the lack of oversight and the retention of information gathered by the team. used the example of "junior enlisted team members having access to information that may have had an affair" as an example of an area in which the team may have overstepped its authority. also cited a It was in this context that the discussion about oversight and data retention took place.

~~(S//NF)~~ In the time frame started to look into Red Team activities and discovered there was no clear policy on data retention. He found that various teams were keeping information collected from operations He was "blown away" by the lack of oversight within regarding the collection, access, and retention of information. This information was stored on shared drives with no auditing or oversight as to "who was accessing the information and why it was being retained." With extensive experience in the Signals Intelligence Directorate, he thought the Red Teams were inappropriately handling data. He held meetings with managers, including Red Team managers, to make it clear that the organization "needed to be more professional in the way data was handled and retained." It would not have surprised him if went back to the Red Team and ordered the deletion of information pertaining to He did not specifically order to delete information pertaining to but he was so "spun up" about the lack of oversight and policy on data retention that his message to management could definitely have led to someone ordering the deleting of data. He also told the managers they needed to remove operator accesses to computers no longer required for legitimate operations.

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ claimed that he was never shown the analyst report prepared on and was never told that may have inappropriately released classified information about Had actually "passed" classified information on the unclassified network, the team should have created a SAR and reported that event as an unauthorized disclosure of classified information so that "could clean up the network." If the analysts had written a report on this issue he assumed the report would have been "passed along."

(b)(3)-P.L. 86-36

~~(S//NF)~~ told that the analysts thought was having an affair with and that he had not changed his computer password He was told the analysts thought there was a potential UCMJ violation and should be held accountable. opined that "it was his experience that there needed to be other charges present; not just infidelity, for action to be taken against an officer for infidelity."

~~(S//NF)~~ did not see any of the screen shots the team had collected on that led the analysts to think that he was having an affair with He understood the issue with to be limited to an allegation of infidelity and "he did not want to see any information about an alleged affair."

(U//~~FOUO~~) Team operators go through a lengthy technical training process before being assigned to an operation. The training is centered on the technical aspects of the job. There is

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

(b)(6)

(b)(1)
(b)(3)-P.L. 86-36

little, if any, training on reporting requirements. There is a close relationship with the NSA OGC for operations approval, but the OGC did not provide training on external reporting requirements. The training provided by OGC to SID was much more detailed than the training provided to IAD.

(b)(3)-P.L. 86-36

(b)(6)

(U//~~FOUO~~)

(U//~~FOUO~~) was interviewed on 1 March 2013 and provided the following sworn testimony.

(U//~~FOUO~~) has been assigned to the Joint Communications Monitoring Activity (JCMA) since and has been the JCMA Her duties include reviewing all JCMA reports.

(~~S//NF~~) The JCMA did not monitor the email communications between No reports were made or files created concerning their email correspondence.

(~~S//NF~~) JCMA procedures do not allow monitoring of communications absent a specific tasking order. The JCMA did not monitor the email communications between No reports were made or files created concerning their email correspondence.

(U//~~FOUO~~)

(U//~~FOUO~~) was interviewed on 1 March 2013 and provided the following sworn testimony.

(U//~~FOUO~~) has been assigned to the Joint Communications Monitoring Activity (JCMA) and has been JCMA

(~~S//NF~~) The JCMA mission is

(~~S//NF~~) While emails and

JCMA did not write reports or conduct an analysis of any communications .

(~~S//NF~~) In the timeframe the JCMA was asked to check if any communications had been stored or retained. This request came from and IAD. A search was conducted that revealed no emails, files, or reports in any JCMA repository.

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

(b)(1)
(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08622

V. (U) Analysis and Conclusions

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) **Failure to report to appropriate authorities possible violations of federal criminal law as required by NSA/CSS Policy 5-5, *Reporting of Security Incidents and Criminal Violations***

(U//~~FOUO~~) NSA/CSS Policy 5-5, *Reporting of Security Incidents and Criminal Violations*, requires that "possible criminal acts committed by non-affiliates and discovered by affiliates while on official duty" shall be reported to the NSA/CSS Associate Directorate for Security and CounterIntelligence. However, this policy states that "[v]iolations of law discovered through COMSEC monitoring shall be reported in a manner consistent with" NTISSD No. 600. Because the Red Team Operations outlined in this report were conducted, at least in part, under COMSEC Monitoring authorities[1], any potential violation of law discovered during the Red Team's [redacted] fell outside NSA/CSS Policy 5-5 and reporting was not required under that policy.

(U//~~FOUO~~) **Failure to report information related to a significant crime to a military commander or law enforcement agency with appropriate jurisdiction as required by NTISSD No. 600**

~~(S//NF)~~ NTISSD No. 600 states that "information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having appropriate jurisdiction." The information that was evidence of possible criminal activity by [redacted] was acquired incidentally from government telecommunications during the course of authorized monitoring. However, the possible criminal activity – adultery and the potential compromise of classified material resulting from having classified material on an unclassified computer – does not constitute "significant crime".[2] Therefore, because [redacted] possible criminal activity was not a significant crime, there was no requirement to report it under NTISSD No. 600.

---

[1] (U//~~FOUO~~) *See* NSA Red Team Standing Rules of Engagement, which states that "[u]nder the authority of National Security Directive 42 . . . and in conformance with . . . [DoD Instruction 8560.01, Communications Security (COMSEC) Monitoring and Information Assurance Readiness Testing], the NSA Red Team performs readiness and vulnerability testing of DoD national security systems."

[2] (U//~~FOUO~~) "Significant crime" is not further defined in NTISSD No. 600. However, the 1995 Memorandum of Understanding regarding Reporting of Information Concerning Federal Crimes, to which the Attorney General and NSA are parties, defines "serious felony offenses" as crimes involving intentional infliction or threat of death or serious physical harm; crimes, including acts of terrorism, that are likely to affect the national security, defense or foreign relations of the U.S., crimes involving unauthorized electronic surveillance in the U.S., violations of U.S. drug laws; and the transmittal, investment and/or laundering of proceedings of these types of unlawful activities.

Release: 2019-06
NSA:08623

(U//~~FOUO~~) **Failure to ensure that the Red Team took required actions to report and respond to incidents as required by Red Team SOP**

(U//~~FOUO~~) The [redacted] Red Team SOP, *Incident Response and Activity Documentation,* "identifies the appropriate steps for reporting incidents outside of normal activities." All Red Team affiliates are required to be familiar with the document and must review the document at least annually. Paragraph 2 of the SOP notes that, in the normal course of operations, "Red Team members may observe activity or an event that requires additional reporting." The SOP then establishes definitions, triggers, necessary steps, and responsibilities for handling such reportable incidents and significant activity.

(U//~~FOUO~~) Section 4 of the SOP identifies eight activities that, if discovered during Red Team Operations, trigger an "incident response." Including in the list of eight are the discovery of material that exceeds the host's classification level and the discovery of material that may indicate criminal activity or misuse of Government information systems. Paragraph 4 provides descriptions (and flow charts) of the specific actions to be taken if an incident response is required.

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) When information is discovered that exceeds the host's classification level, also referred to as "spillage," the Red Team is required to produce a Significant Activity Report (SAR), including copying the US Cyber Command integree if the material is found on a DoD system, document the incident in the watch log, and report the incident to the client/system owner. Under [redacted] was the client.

(S//NF) During [redacted] the Red Team discovered potentially classified material on [redacted] unclassified computer system. [redacted] Red Team Team [redacted] testified that he reported to his leadership, including [redacted] and [redacted] on multiple occasions that Red Team operators had seen emails from [redacted] on the unclassified network that contained potentially classified information about [redacted] and [redacted] prepared a report that described the potentially classified information found on [redacted] unclassified computer. [redacted] recalled sending the report to [redacted] and discussing it with him. Although the Red Team management, up to and including [redacted] was aware of the potentially classified information found on [redacted] unclassified computer, no SAR was completed, US Cyber Command was not notified, and the incidents were not reported to [redacted] or the system owner, all in violation of the SOP. Although [redacted] testified that he first saw the report containing this information in [redacted] he acknowledged that it was possible that [redacted] had sent him this report in 2011, but he hadn't received it or failed to read it. Given the wealth of testimony that [redacted] was informed orally and in writing, we conclude by a preponderance of the evidence that [redacted] had been informed that potentially classified material was found on [redacted] unclassified computer and that he failed to ensure that the Red Team SOP was followed.[3]

(b)(6)

(b)(3)-P.L. 86-36
(b)(6)

[3] (U//~~FOUO~~) It is important to note that the SOP, dated 14 June 2010, was approved by [redacted] himself.

(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08624

~~(S//NF)~~ Separately, paragraph 4.e of the SOP delineates similar actions when material is discovered that may indicate criminal activity or misuse of Government information systems. In addition to submitting a SAR, these required actions include notifying "legal" and writing a report. It is undisputed that Red Team members discovered, and informed their chain of command up to and including [redacted] information that led them to believe that [redacted] may have been engaged in adultery with [redacted] Adultery, when service discrediting or prejudicial to good order and discipline, is criminal activity under the Uniform Code of Military Justice (Article 134) which applies to members of the armed services, including [redacted] Despite this, and in violation of the Red Team SOP, [redacted] decided not to report this activity through the use of a SAR and he decided not to report this activity to the Office of General Counsel. [redacted] decision to not report this information, supported by his supervisor [redacted] deprived senior military and civilian leaders of the opportunity to determine whether this information was relevant and required any action on their part.

(U//~~FOUO~~) **Failure to report information, or ensure the information was reported, to the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)) as required by DTM 08-052.**

(b)(3)-P.L. 86-36

~~(S//NF)~~ DTM 08-052, DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters, requires that DoD components report certain circumstances "involving an intelligence activity or intelligence personnel." DTM 08-052 incorporates the Executive Order 12333 definition of an "Intelligence Activity": "all activities that elements of the Intelligence Community [including NSA] are authorized to conduct pursuant to this order." EO12333 authorizes NSA to conduct eight specific activities, including the Director acting as the National Manager for National Security Systems, a role IAD fills. Red Team activities are part of IADs responsibilities. Therefore, for the purposes of determining the applicability of DTM 08-052, the focus is on the activities conducted by NSA's Red Team. Furthermore, [redacted] is not considered "intelligence personnel." Because nothing the RED Team did with regard to [redacted] under the [redacted] operation was inappropriate and [redacted] was not intelligence personnel, there was no requirement for [redacted] or anyone associated with the Red Team to report under DTM 08-052.[4]

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

[4] ~~(S//NF)~~ NSA may have been aware of an affair between [redacted] and [redacted] before that [redacted] the Agency was required to report, and did report the matter through the OIG to ATSD(IO).

Release: 2019-06
NSA:08625

(b)(3)-P.L. 86-36
(b)(6)

IV. (U) RESPONSE TO TENTATIVE CONCLUSIONS

(U//~~FOUO~~) Tentative conclusions were forwarded to [redacted] on 18 March 2014. [redacted] responded to the OIG's tentative conclusions via email on 20 March 2014. His response is attached (Appendix H).

(U//~~FOUO~~) The OIG reviewed the response provided by [redacted] and determined that his response did not have an impact upon the conclusions.

Release: 2019-06
NSA:08626

(b)(3)-P.L. 86-36
(b)(6)

V. (U) CONCLUSION

~~(S//NF)~~ The preponderance of the evidence supports the conclusion that [redacted] retired, failed to ensure that the Red Team took required actions to report and respond to incidents the Red Team SOP requires after he was informed that [redacted] may have been involved in criminal activity by engaging in adultery in violation of UCMJ article 134 and that [redacted] inappropriately maintained and passed potentially classified information through an unclassified computer network.

(U//~~FOUO~~) We conclude that [redacted] did not violate NSA/CSS Policy 5-5, *Reporting of Security Incidents and Criminal Violations*, because Red Team operations are conducted, in part, under COMSEC Monitoring authorities and any violation discovered during the Red Team's [redacted] operation fell outside NSA/CSS Policy 5-5.

~~(S//NF)~~ We conclude that [redacted] did not violate NTISSD No. 600 reporting requirements for "significant crime" because the possible criminal activity, a violation of UCMJ article 134, – adultery – does not constitute a significant crime.

~~(S//NF)~~ We concluded that [redacted] did not violate the reporting requirements of DTM 08-052, *DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters*, because the Red Team acted within their scope of authority and [redacted] was not an intelligence official at that time.

(b)(1)
(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08627

VI. (U) DISTRIBUTION OF RESULTS

(U//~~FOUO~~) This report of investigation will be provided to:

1. M/ER for information and any appropriate action
2. Associate Directorate for Security and Counter Intelligence (Q234)
3. Department of Defense Inspector General
4. [redacted] (b) (6)

(U//~~FOUO~~) A summary of this report of investigation will be provided to:

1. NSA Office of General Counsel

[redacted]
Senior Investigator

(b) (3)-P.L. 86-36

Concurred by:

[redacted]
Assistant Inspector General
for
Investigations

Release: 2019-06
NSA:08628

Appendix A

(U) Applicable Authorities

(b)(3)-P.L. 86-36

(U) NSA/CSS Policy 5-5, REPORTING OF SECURITY INCIDENTS and CRIMINAL VIOLATIONS

5. (U//~~FOUO~~) Any incident described below shall be reported to ADS&CI or, if after normal duty hours, to the Security Operations Command Center

b. (U//~~FOUO~~) Possible criminal acts committed by non-affiliates and discovered by affiliates while on official duty.

(b)(6)

(U) Title 10, U.S. Code §934 (Uniform Code of Military Justice, Article 134)

Though not specifically mentioned in this chapter, all disorders and neglects to the prejudice of good order and discipline in the armed forces, all conduct of a nature to bring discredit upon the armed forces, and crimes and offenses not capital, of which persons subject to this chapter may be guilty, shall be taken cognizance of a general, special or summary court-martial, according to the nature and degree of the offense, and shall be punished at the discretion of that court.

(U) Punitive Articles of the UCMJ, Article 134 – Adultery

Elements.

(1) That the accused wrongfully had sexual intercourse with a certain person;

(2) That, at the time, the accused of the other person was married to someone else; and

Release: 2019-06
NSA:08629

(3) That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

(U) Directive-Type Memorandum (DTM) 08-052 – DoD Guidance for Reporting Questionable Intelligence Activities and Significant or Highly Sensitive Matters

1. REPORTING PARAMETERS
a. The DoD Components shall report the following matters to the Assistant to the Secretary of Defense for Intelligence Oversight ATSD(IO) in accordance with references (a) and (d).
5. Significant or Highly Sensitive Matters. A development or circumstance involving an intelligence activity or intelligence personnel that could impugn the reputation or integrity of the DoD Intelligence Community or otherwise call into question the propriety of an intelligence activity. Such matters might be manifested in or by an activity:

(a) Involving congressional inquiries or investigations.
(b) That may result in adverse media coverage.
(d) Related to the unauthorized disclosure of classified or protected information, such as information identifying a sensitive source and method. Reporting under this paragraph does not include reporting of routine security violations.

(U//~~FOUO~~) NTISSD No. 600, Communications Security (COMSEC) Monitoring

(U//~~FOUO~~) Information acquired incidentally from government telecommunications during the course of authorized COMSEC monitoring which relates directly to a significant crime will be referred to the military commander or law enforcement agency having the appropriate jurisdiction.

(U//~~FOUO~~) NSA IAD [redacted] Red Team SOP, Incident Response and Activity Documentation

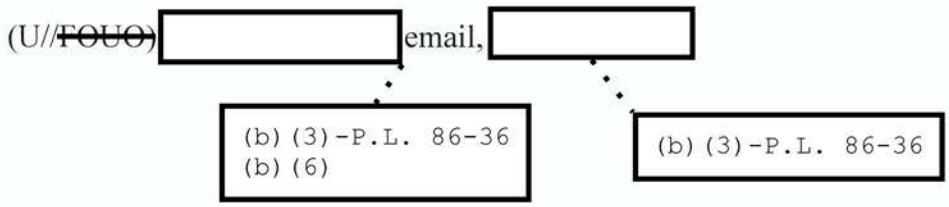
2. (U//~~FOUO~~) Overview of Incident Response and Significant Activity Report
a. (U//~~FOUO~~) In the course of normal operations, Red Team members may observe activity or an event that requires additional reporting. The following sections establish definitions, triggers, necessary steps and responsibilities for handling reportable incidents and significant activity.

(b)(3)-P.L. 86-36

(U//~~FOUO~~) Section 4, INCIDENT RESPONSE
a. (U//~~FOUO~~) Within the broad range of activities that Red Team identifies as "significant activity" there are some events that are also identified as reportable incidents. Incidents require specific responses in addition to the generation of a SAR; detailed steps are listed in the following sections. Each of the following is an incident response trigger:
3) Material is discovered exceeding the host's classification level
4) Material is discovered that may indicate criminal activity or misuse of Government information systems.

Release: 2019-06
NSA:08630

Appendix B



Release: 2019-06
NSA:08631

~~SECRET//NOFORN~~

[redacted]

From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: FW: (U) NSA Red Team Targeting
Attachments: Timeline [redacted] (2).docx
Signed By: [redacted]

Classification: [redacted]

[redacted]

Regards,

[redacted]

(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36

From: [redacted]
Sent: [redacted]
To: [redacted]
Cc: [redacted]
Subject: FW: (U) NSA Red Team Targeting

Classification: [redacted]

FYSA

[redacted]

(b) (3)-P.L. 86-36
(b) (6)

From: [redacted]
Sent: [redacted]
To: Plunkett Debora A NSA-I USA CIV
Cc: [redacted]
Subject: (U) NSA Red Team Targeting

Classification: [redacted]

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08632

~~SECRET//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36

As requested, the attached timeline and mitigation recommendations concerning the are provided.

Earlier today, after discussing the matter with our POC, I notified and his staff as well as about the accesses obtained on systems. I also double-checked with JCMA to see if they had obtained anything related to this in their efforts supporting – They had not.

V/R,

(b) (3)-P.L. 86-36

(b) (6)

(b) (3)-P.L. 86-36
(b) (6)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On:

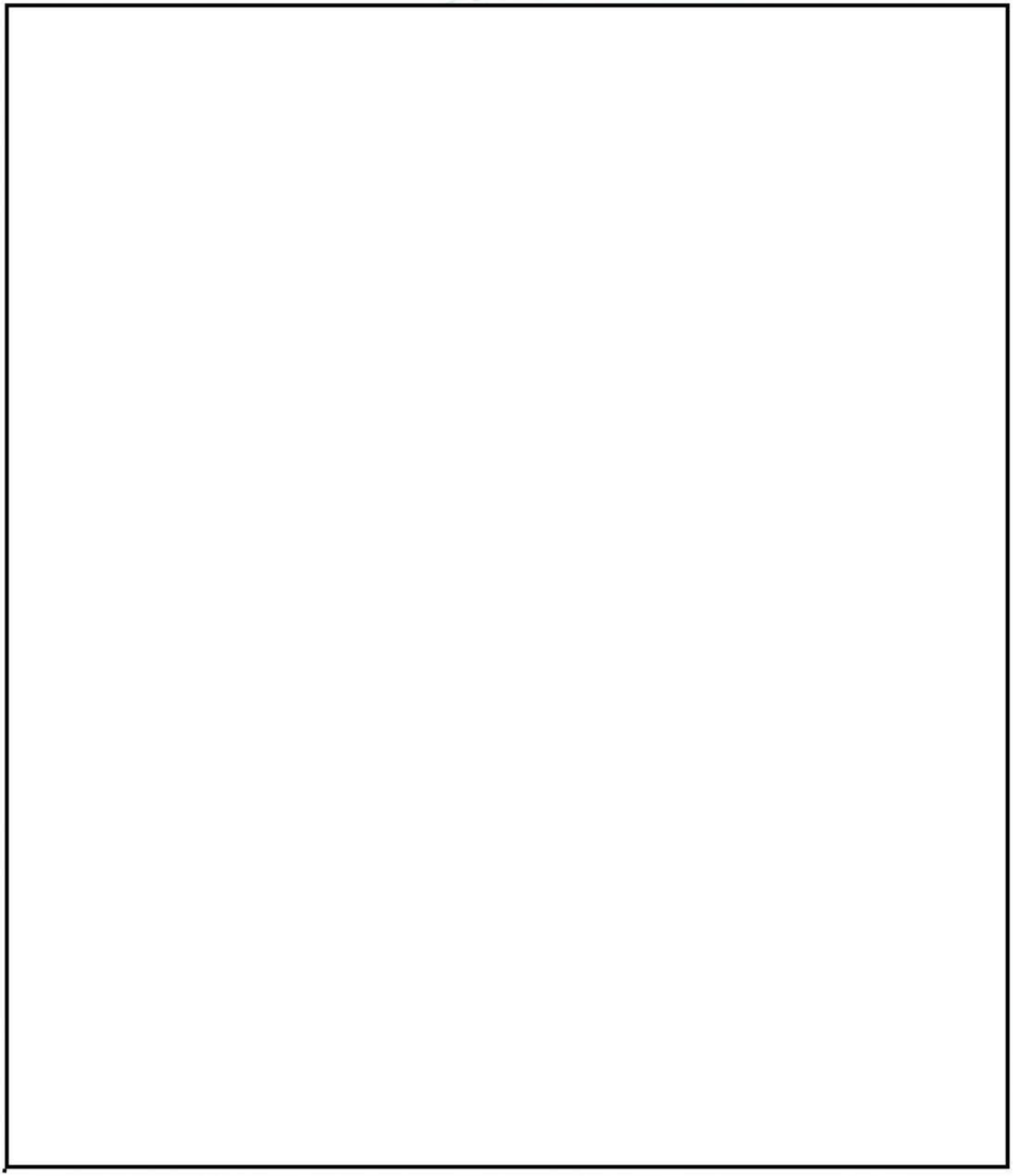
Classification: ~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08633

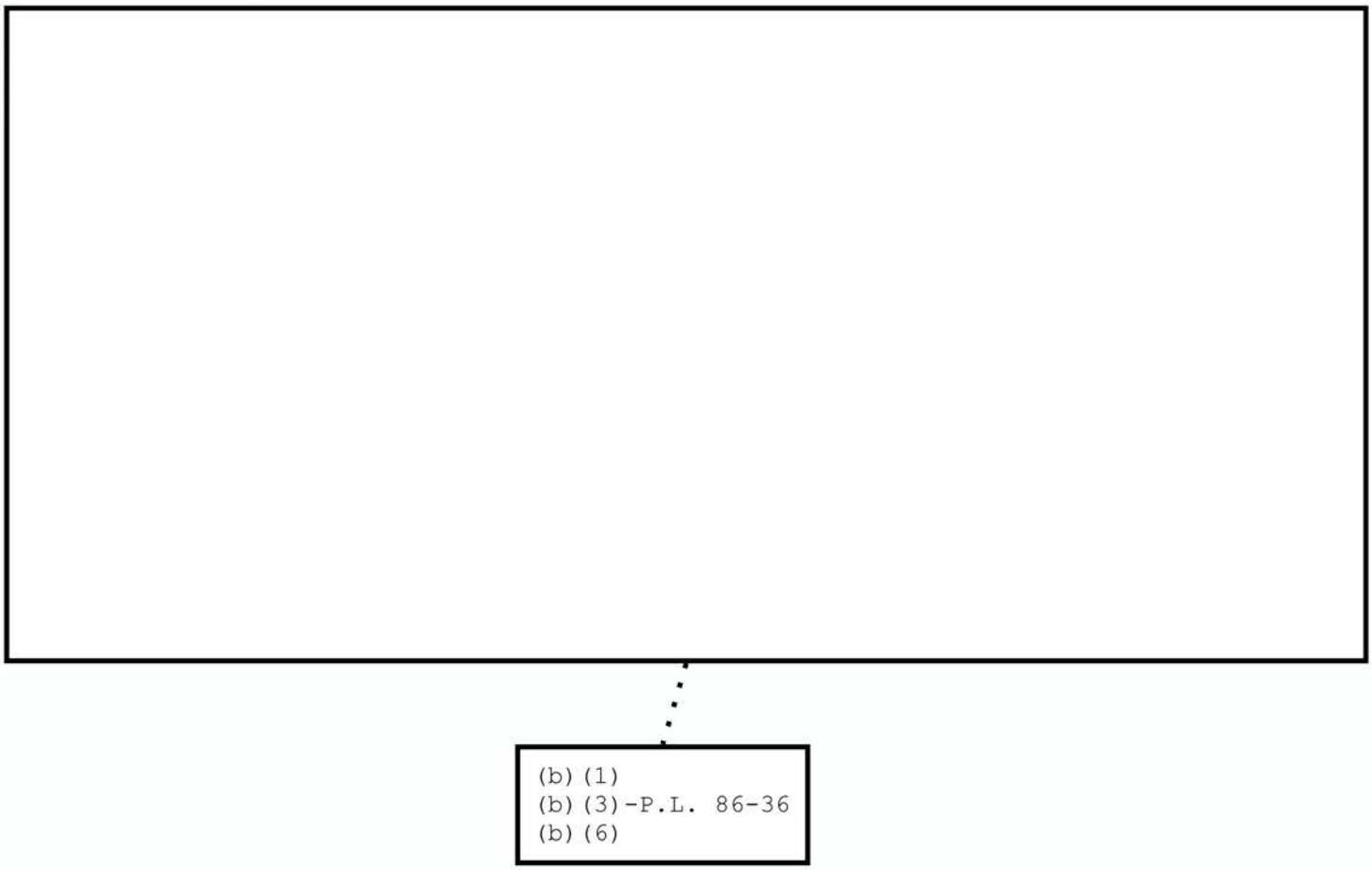
(b) (1)
(b) (3)-P.L. 86-36

~~(S//NF)~~ Operation [redacted] NIPR exploitation timeline:



(b) (1)
(b) (3)-P.L. 86-36
(b) (6)

Declassified and Approved for Release by NSA on 07-31-2018 pursuant to E.O. 13526
Declassify On: 20701108



(b)(1)
(b)(3)-P.L. 86-36
(b)(6)

Appendix C

(U) Red Team Analyst Report, 20 July 2011

Release: 2019-06
NSA:08636

SECRET//NOFORN

24

From:
Sent:
To:
Cc:
Subject: (U) FW: Final Report on access
Attachments:

Importance: High

(b) (1)
(b) (3)-P.L. 86-36

Classification: SECRET//NOFORN

Attached is the original email sent from the and I. I haven't found it yet, but I sent you an edited version of this below. You can see the timeframe is July.

(b) (3)-P.L. 86-36
(b) (6)

Regards,

(U//FOUO)

(b) (3)-P.L. 86-36

From:
Sent: Wednesday, July 20, 2011 7:25 AM
To:
Cc:
Subject: FW: Final Report on access
Importance: High

With supporting files..

From:
Sent: Wednesday, July 20, 2011 7:19 AM
To:
Cc:
Subject: Final Report on access
Importance: High

(b) (3)-P.L. 86-36

Below is a summary of all the intelligence gained from the our access with details on how a FIS would take advantage of these vulnerabilities.

Please let or myself know if you require further details.

(b) (1)
(b) (3)-P.L. 86-36

SECRET//NOFORN

Release: 2019-06
NSA:08637

(b)(3)-P.L. 86-36

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

1. ~~(S//NF)~~ **Executive Summary:** Following is a synopsis of Intelligence data mined from NIPRNet Access of

Release: 2019-06
NSA:08638

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08639

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08640

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08641

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6) NSA:08642

Release: 2019-06

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08643

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08644

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08645

Doc ID: 6672264

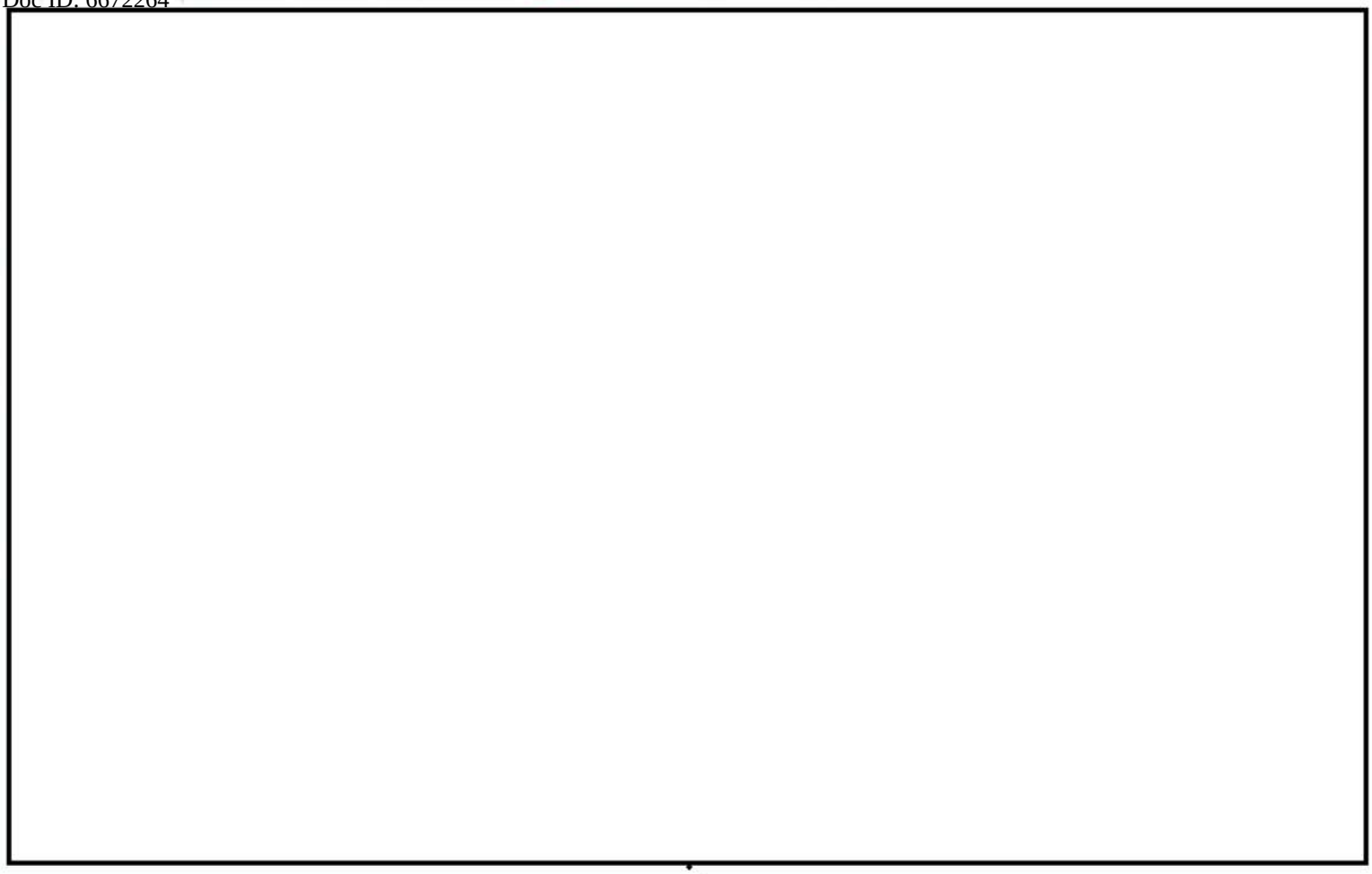
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08646

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08647



(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08648

APPENDIX D

(U//FOUO)

(b)(1)
(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08649

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIF

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIF

Release: 2019-06
NSA:08651

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIF

Release: 2019-06
NSA:08652

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIF

Release: 2019-06
NSA:08653

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(7)(E)

DIF

Release: 2019-06
NSA:08654

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(7)(E)

DIE

Release: 2019-06
NSA:08655

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(7)(E)

DIE

Release: 2019-06
NSA:08656

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIF

Release: 2019-06
NSA:08657

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36

DIE

Release: 2019-06
NSA:08658

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)
(b)(7)(E)

DIE

Release: 2019-06
NSA:08659

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)
(b)(7)(E)

DIE

Doc ID: 6672264

APPENDIX E

(U) Red Team SOP, Incident Response and Activity Documentation (14 June 2010)

Release: 2019-06
NSA:08661

Doc ID: 6672264

National Security Agency
Information Assurance Directorate

NATIONAL SECURITY AGENCY

[redacted] Red Team SOP

Incident Response

and

Activity Documentation

(b)(3)-P.L. 86-36

Serial [redacted]-011-10
Date: 14 June 2010

Release: 2019-06
NSA:08662

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

(U) INCIDENT RESPONSE AND ACTIVITY DOCUMENTATION SOP

Reviewed By:

[redacted]

Chief, [redacted]

[redacted]

for

Associate General Counsel (Information Assurance)

[redacted]

IAD Oversight & Compliance (IV)

(b) (3)-P.L. 86-36

Approved By:

[redacted]

(b) (3)-P.L. 86-36
(b) (6)

DISTRIBUTION: [redacted] IV: [redacted]

(U) This document (IA Serial No. [redacted]-011-10) supersedes documents [redacted]-024-09, "Incident Response", and [redacted]025-09, "Operational Reporting".
(U) OPI [redacted] 968-6625s.
(U) No section of this document shall be released without approval from [redacted]

Release: 2019-06
NSA:08663

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

(U) PURPOSE AND SCOPE

(U//~~FOUO~~) This document describes the operational activity documentation requirements during normal NSA Red Team operations, and identifies the appropriate steps for reporting incidents outside of normal activities.

(U//~~FOUO~~) This SOP is intended primarily for the Operations branch, but all Red Team affiliates must be familiar with this document. Steps that affect all Red Team affiliates are outlined in sections **3 (Significant Activity Reports), 4.d. (Incident Response- Material is discovered that may indicate criminal activity or misuse of Government information systems) and 4.h. (Incident Response- Evidence of an unauthorized intruder is discovered on Red Team systems).** All Red Team affiliates shall review this document at least annually, as outlined in the *Critical Documentation* SOP.

(U//~~FOUO~~) This document does not apply to deconflictions (i.e., the process by which one verifies whether or not suspicious activity detected on a U. S. Government or military network is attributable to the NSA Red Team), which are covered in the SOP titled *Deconflictions* [redacted]-007-10). For instructions on deconfliction reporting and responding to incidents related to deconflictions, refer to the *Deconflictions* SOP.

(U//~~FOUO~~) This document does not apply to [redacted] which are covered in the SOP titled [redacted] For instructions on [redacted] reporting and responding to incidents related to [redacted] refer to the [redacted] SOP (that document supersedes this SOP).

(U//~~FOUO~~) In this document, section 4, *Incident Response*, and section 5, *Oversight & Compliance*, implement the requirements of References c and d.

Release: 2019-06
NSA:08664

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

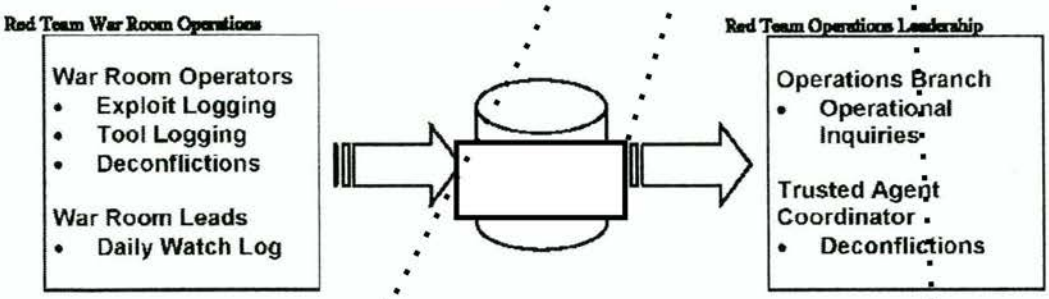
(U) STANDARD OPERATING PROCEDURES

(b)(3)-P.L. 86-36

1. (U//~~FOUO~~) [redacted] Operations Database

a. (U//~~FOUO~~) All pertinent details for any operational activity shall be entered into the operations support database, [redacted]. This database is used to track critical information for every operational event, such as: date and time, IP addresses, all target identification, and a summary of activities carried out on the target system [redacted]. All of this information must be entered in [redacted] so that Red Team operations can be properly audited at any time. [redacted] data is also used in the process of deconfliction, and for clean-up of [redacted]. Note- *Even an unsuccessful attack or other operational event may be subject to deconfliction and, therefore, must be properly recorded.* [redacted] database is also used to support [redacted] Security Solutions and NSA/CSS Threat Operations Center (NTOC) missions.

Flow Diagram- [redacted] Red Team Operations Database



(U//~~FOUO~~) Figure 1.a

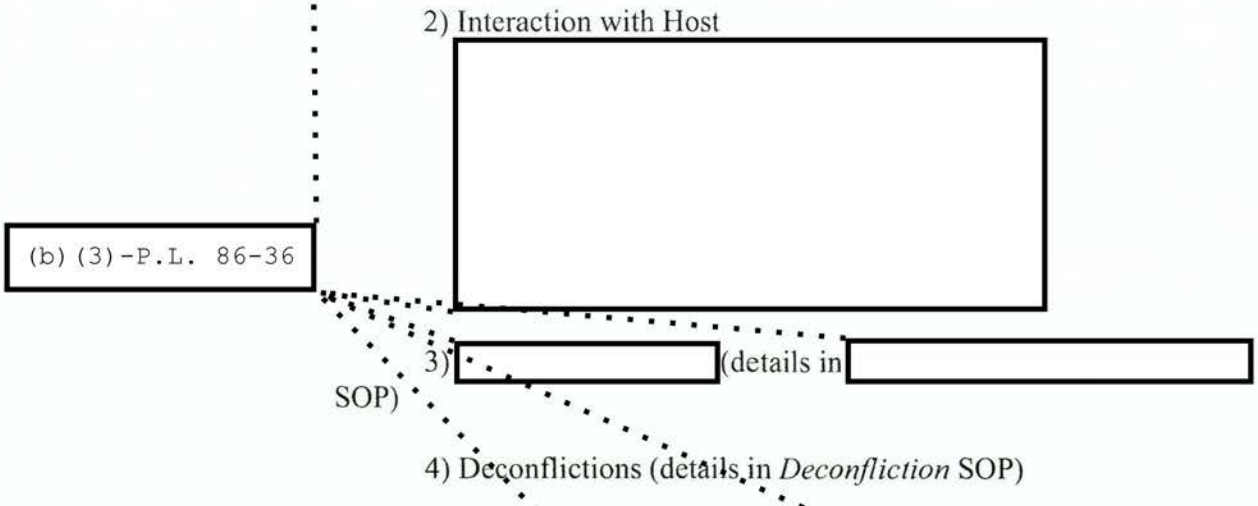
b. (U//~~FOUO~~) Each War Room operator shall log daily activities in the [redacted] database. Examples of entries include, but are not limited to:

1) Host Details

[redacted]

Release: 2019-06
NSA:08665

Doc ID: 6672264



c. (U//~~FOUO~~) Team Leads shall use the [redacted] Daily Watch Log to record problems, events, and courses of action within their War Room. Examples of entries include, but are not limited to:

- Overview of shift activity
- Tasks to be completed by the next watch
- Open Source Research (focus; results)
- Changes to operations that impact the ongoing activity, with the reason(s) for the change
- Any other items deemed necessary by the Team Lead or Red Team leadership

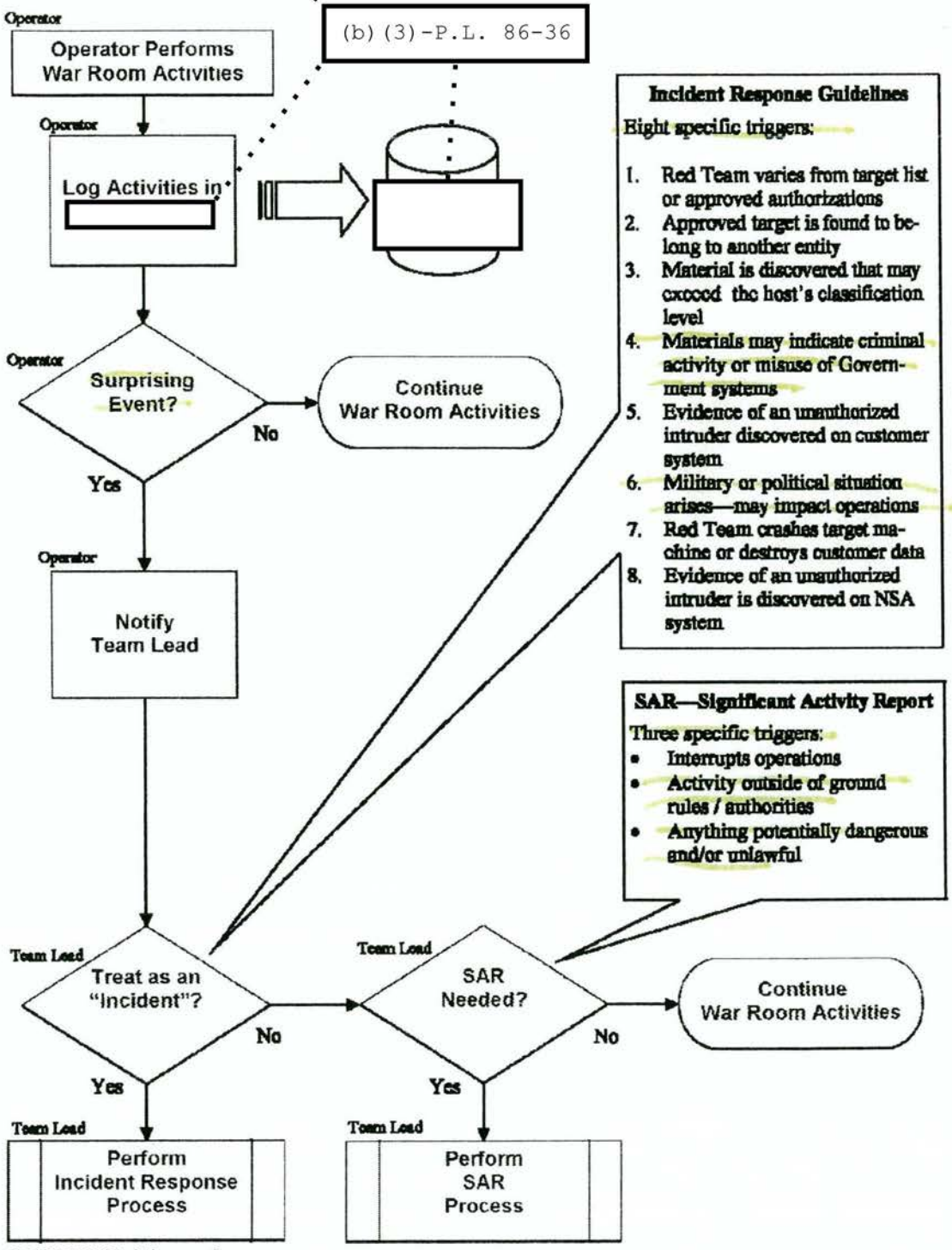
d. (U//~~FOUO~~) Each War Room Team Lead is responsible for ensuring all pertinent War Room activities are properly entered into the [redacted] database.

2. (U//~~FOUO~~) Overview of Incident Response and Significant Activity Report

a. (U//~~FOUO~~) In the course of normal operations, Red Team members may observe activity or an event that requires additional reporting. The following sections establish definitions, triggers, necessary steps and responsibilities for handling reportable incidents and significant activity.

Release: 2019-06
NSA:08666

Flow Diagram—Overview of Incident Response & Significant Activity Report



(U//~~FOUO~~) Figure 2

Release: 2019-06
NSA:08667

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

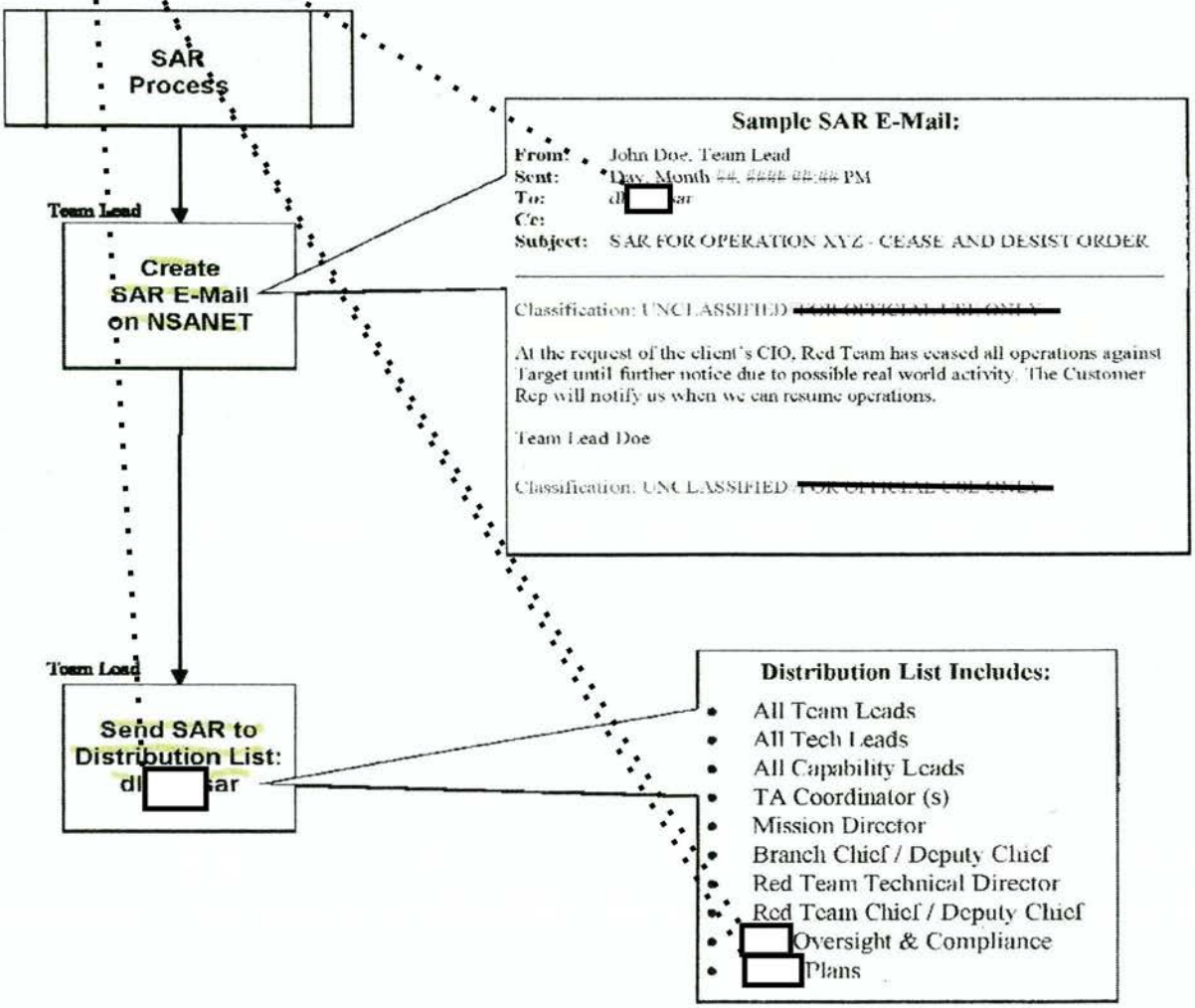
3. (U//~~FOUO~~) Significant Activity Report (SAR)

a. (U//~~FOUO~~) The Red Team defines significant activity as: any activity that interrupts or prohibits normal operations; any activity outside the scope of Red Team authorities; or any activity that uncovers something potentially unlawful or harmful. Whenever significant activity takes place during a Red Team operation, a Team Lead will prepare a SAR to inform the operational chain of command. Examples of significant activities include, but are not limited to:

1) Red Team becomes Non-Mission Capable
2) Discovery of any unauthorized network activity
3) Change in the hours of operation
4) Request to cease operations (Cease and Desist Order)
5) Any other event that could impact Red Team operations

(b)(3)-P.L. 86-36

Flow Diagram—Significant Activity Report (SAR)



(U//~~FOUO~~) Figure 3.a

Release: 2019-06
NSA:08668

Doc ID: 6672264

b. (U//~~FOUO~~) Red Team Services shall develop and maintain an e-mail distribution list on NSANET, named "dl [redacted] sar", that shall be used to distribute SARs. This list shall include, at a minimum:

1) All Team Leads
2) All Tech Leads
3) All Capability Leads
4) Trusted Agent Coordinator(s)
5) Mission Director
6) Operations Branch Chief / Deputy Chief
7) Red Team Technical Director
8) Red Team Chief / Deputy Chief
9) [redacted] Oversight & Compliance
10) [redacted] Plans

(b)(3)-P.L. 86-36

c. (U//~~FOUO~~) The SAR shall take the form of an e-mail sent on NSANET to the "dl [redacted] sar" distribution list. The message shall contain the following information: a clear description of the activity that initiated the SAR, who was involved, when and where the incident occurred, and any actions taken. A sample SAR can be found in Appendix A.

d. (U//~~FOUO~~) Additional SAR recipients shall be added to the e-mail, as appropriate. Examples include, but are not limited to:

1) [redacted] shall be included if the SAR is about systems/access issues
2) Red Team Services leadership shall be included if the SAR is about training/capability gaps
3) ASR leadership shall be included if the SAR is about tool failure
4) [redacted] leadership shall be included if the SAR is about Red Team being [redacted]
5) NSA/CSS Threat Operations Center (NTOC) and USCYBERCOM LNO shall be included if the SAR is about discovery of significant vulnerability or analytic finding on any DoD system. [redacted] TD shall provide direction whether or not to use the NTOC reporting tool, [redacted]
6) US-CERT shall be included if the SAR is about discovery of significant vulnerability or analytic finding on any non-DoD system (e.g. USSS.gov., DOE.gov., USCG.mil)
7) Associate General Counsel/Information Assurance (AGC/IA) and IAD Oversight & Compliance (IV) shall be included if the SAR is about any activity beyond the scope of Red Team authorities

e. (U//~~FOUO~~) Red Team branch and division leadership shall determine whether or not to alert NTOC, USCYBERCOM or US-CERT, except as specifically outlined in the Incident Response scenarios listed in section 4 of this document.

Release: 2019-06
NSA:08669

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

4. (U//~~FOUO~~) INCIDENT RESPONSE

a. (U//~~FOUO~~) Within the broad range of activities that Red Team identifies as "significant activity" there are some events that are also identified as reportable incidents. Incidents require specific responses in addition to the generation of a SAR; detailed steps are listed in the following sections. Each of the following is an incident response trigger:

1) Red Team varies from the approved target list or approved authorizations on a network
2) Approved target is found to belong to another entity
3) Material is discovered exceeding the host's classification level
4) Material is discovered that may indicate criminal activity or misuse of Government information systems
5) Evidence of an unauthorized intruder is discovered on customer networks
6) A military/political situation arises that may impact Red Team operations
7) Red Team inadvertently reboots, crashes or destroys data on a target machine
8) Evidence of an unauthorized intruder is discovered on Red Team systems

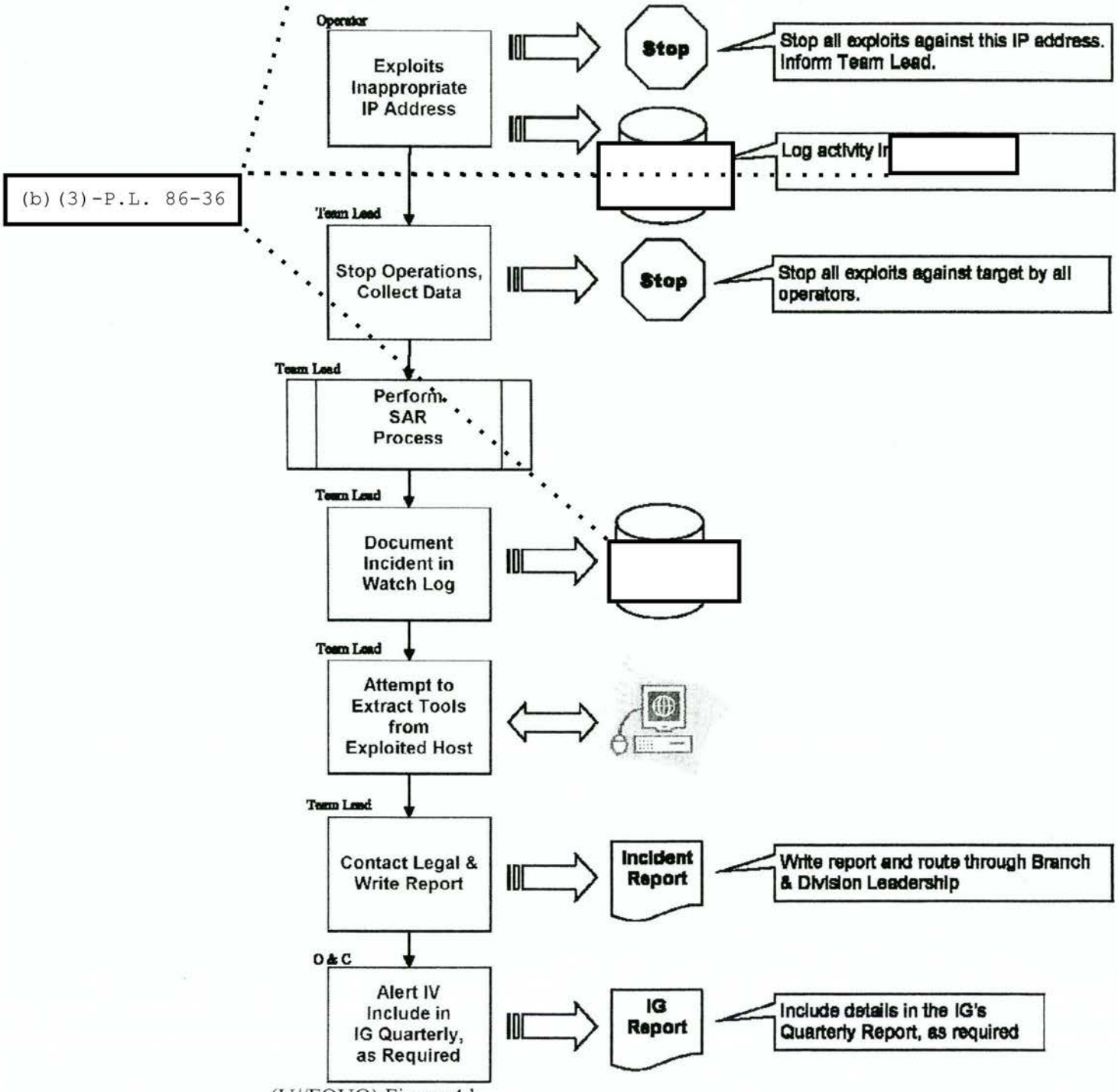
(b)(3)-P.L. 86-36

Note- This is an addendum to the guidance provided in Annex D of Reference c.

Release: 2019-06
NSA:08670

b. (U//~~FOUO~~) Red Team varies from the approved target list

Flow Diagram—Red Team Varies From the Approved Target List



(U//~~FOUO~~) Figure 4.b

Release: 2019-06
NSA:08671

Doc ID: 6672264

IA Serial No [redacted]011-10 Dated: 14 June 2010

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) **Incident:** An operator has mistakenly varied from the target list or approved authorizations on a network, for example by typing an incorrect IP address for a probe or exploit. *Note:* The *target list* is a list of IP addresses provided by the customer or compiled by Red Team through research/target development activities. All addresses on this list have been verified by AGC/IA as falling under the Red Team's legal authority to probe or exploit. Variation from the approved target list results in probing or exploiting a host or network for which the Red Team may have no legal authority and may result in a criminal violation.

2) (U//~~FOUO~~) **Action: Operator** – Cease all operations against the erroneous IP address. Immediately report the incident to the Team Lead for further guidance and log activity in [redacted] Items to be reported are the intended IP address, the incorrect IP address, the account in use (including its IP address), the time of occurrence (Zulu), all operations (probing or attacking) conducted against the incorrect IP address, and the script file or files which document the erroneous activity.

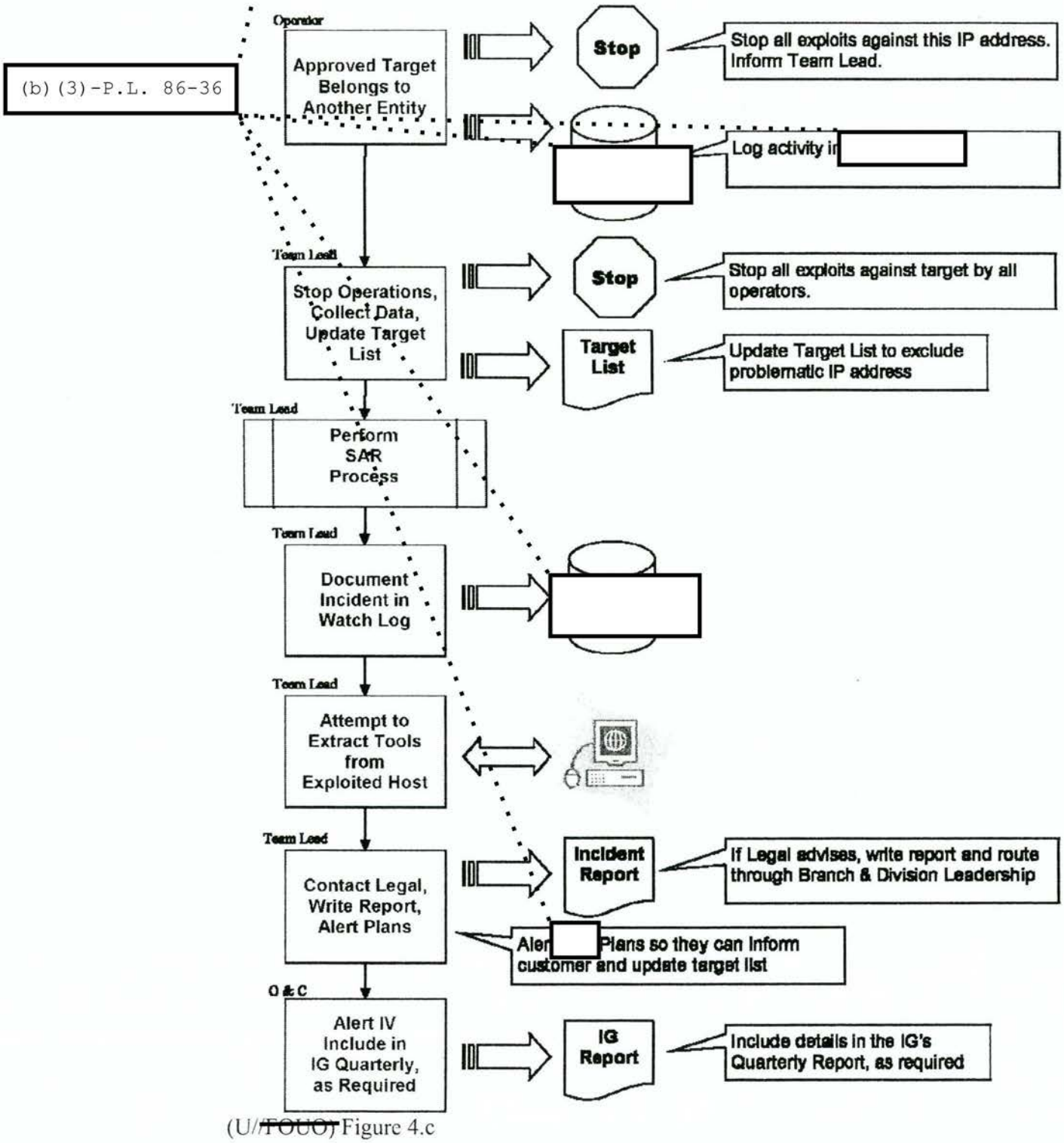
3) (U//~~FOUO~~) **Action: Team Lead** – Ensure that all operations against the erroneous IP address have ceased and will not be resumed. Update target list and document all details provided by the operator into [redacted] with notes in the Daily Watch Log, and generate a Significant Activity Report (SAR). Steps will be taken to determine the ownership of the incorrect IP address, and any damage that may have been inflicted on the unintended target. Steps will be taken to coordinate the removal of any Red Team tools from the affected host. Notify AGC/IA within one business day. A written report of the incident is required and must be routed through Red Team branch and division leadership.

4) (U//~~FOUO~~) [redacted] Oversight & Compliance (O&C) is responsible for alerting IAD Oversight & Compliance (IV) within one business day and ensuring that the incident and all relevant details are included on the Inspector General's quarterly report, as required.

Release: 2019-06
NSA:08672

c. (U//~~FOUO~~) Approved target is found to belong to another entity

Flow Diagram—Approved target is Found to Belong to Another entity



(U//~~FOUO~~) Figure 4.c

Release: 2019-06
NSA:08673

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) **Incident:** After a given IP address which is on the approved target list has been probed or exploited, evidence is discovered indicating that it actually belongs to an entity that the Red Team has no legal authorization to attack.

2) (U//~~FOUO~~) **Action: Operator** – Cease all operations against the affected IP address. Immediately report the incident to the Team Lead for further guidance and log activity in [redacted] Items to be reported are the affected IP address, the account in use (including its IP address), the time of occurrence (Zulu), all operations (probing or exploiting) conducted against the affected IP address, and the script file or files which document the activity

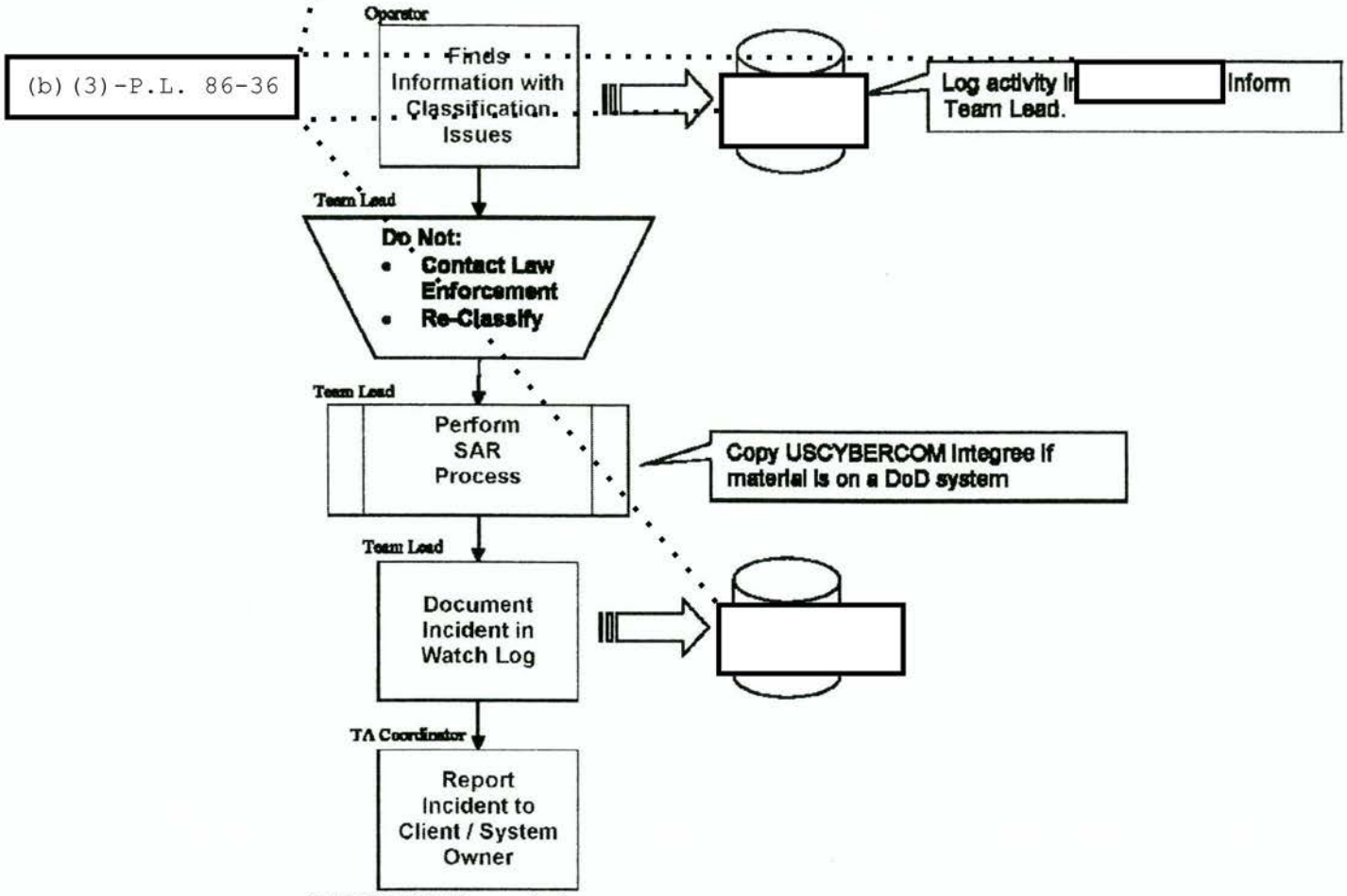
3) (U//~~FOUO~~) **Action: Team Lead** – Ensure that all operations against the affected IP address have ceased and will not be resumed. Document all details provided by the operator into [redacted] under the Daily Watch Log, and generate a Significant Activity Report (SAR). If possible, remove any Red Team tools from the affected host. All Red Team operators are to be informed that the affected IP address or IP address block is off-limits to further operations; this must be logged in [redacted] addressed during shift turnover meetings, and reflected by amendment of the approved target list. Any amended target list must be placed in [redacted] Operations against the affected IP address may be resumed only if it is proven that it belongs to a customer organization legally subject to Red Team attack and the exercise documentation package provides for the inclusion of the IP address. If affected IP address does not belong to a customer organization, alert [redacted] Plans so the target list can be updated. Within one business day, notify AGC(IA) and IV of the incident. A written report of the incident is required, and must be routed through Red Team branch and division leadership

4) (U//~~FOUO~~) [redacted] O&C is responsible for alerting IV and ensuring that the incident and all relevant details are properly documented for inclusion in the Inspector General's quarterly report, as required.

Release: 2019-06
NSA:08674

d. (U//~~FOUO~~) Material is discovered that may exceed the host's classification level

Flow Diagram—Material Discovered, May Exceed Host's Classification Level



(U//~~FOUO~~) Figure 4.d

1) (U//~~FOUO~~) **Incident:** During Red Team operations, a document is discovered whose classification level appears to be higher than that of the host it resides on. *Note:* This situation is sometimes called *spillage*.

2) (U//~~FOUO~~) **General Instructions:** *Do not contact law enforcement*. It is the client's responsibility to control its own information systems, using its own procedures.

3) (U//~~FOUO~~) *Do not attempt to classify the information*. The NSA Red Team is not the originator of the information and, therefore, may not classify it. If the classification is clearly marked on the document, and the content appears consistent with the marking, the marking shall be

Release: 2019-06
NSA:08675

Doc ID: 6672264

considered the classification of the document. If the document is not labeled but it appears that it may contain classified information, the document will be considered "sensitive."

4) (U//~~FOUO~~) **Action: Operator** – Immediately report the incident to the Team Lead, and log activity in [redacted]

(b)(3)-P.L. 86-36

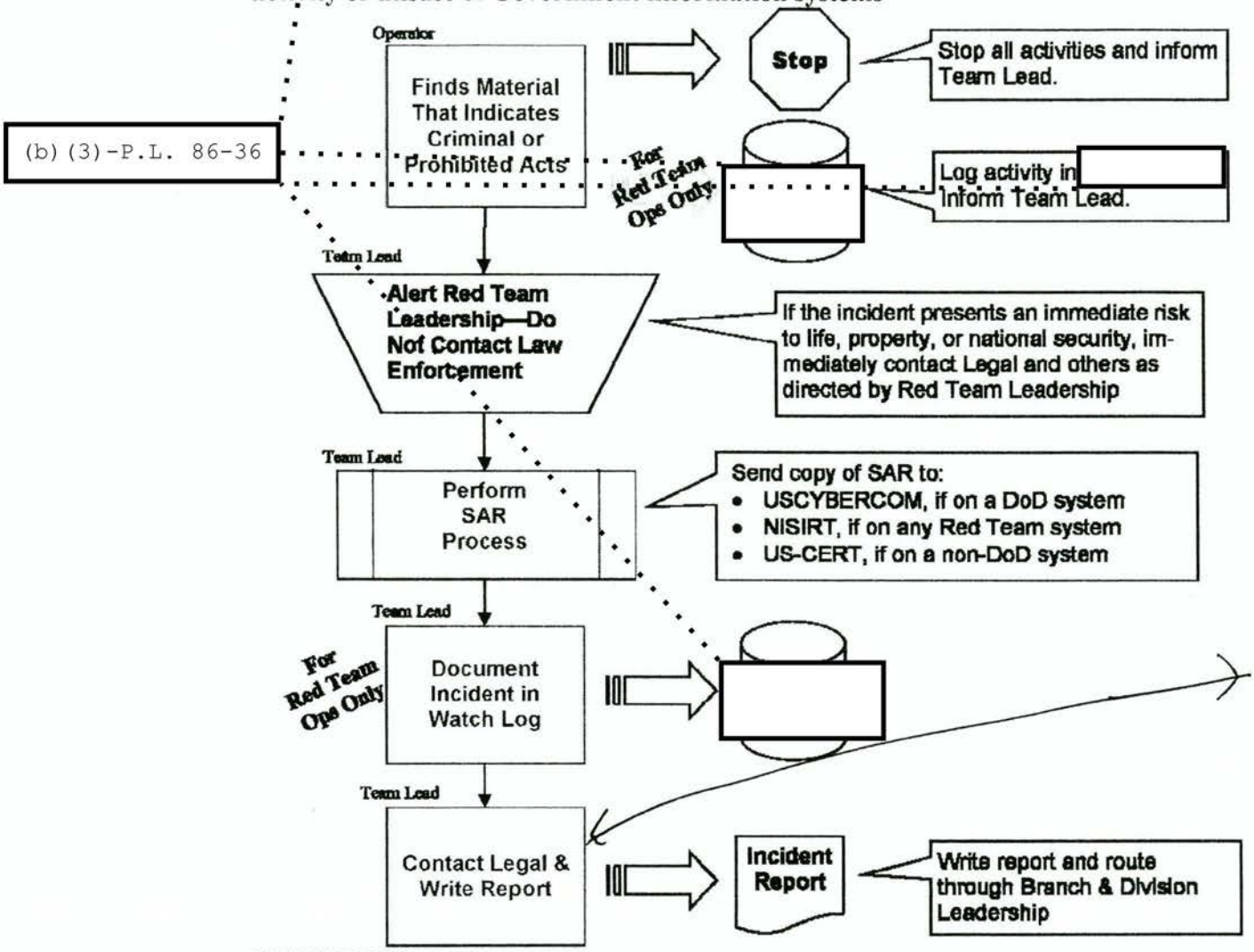
5) (U//~~FOUO~~) **Action: Team Lead** – Document the incident into [redacted] under the Daily Watch Log, and generate a Significant Activity Report (SAR). Relevant details include the date and time (Zulu), the target IP address, and the location of the suspicious information. Forward the SAR to the Red Team USCYBERCOM integree who shall alert the Network Defense Watch Officer (NDWO) and generate a CCIR (Commanders Critical Information Requirement) if appropriate. Operations branch leadership will determine whether or not exploits should be stopped against the target, and will make the determination if and when to remove Red Team tools from the affected host.

6) (U//~~FOUO~~) **Action: TA Coordinator** – If the affected host *is the property of the Red Team's client*, report the incident to the client's Point of Contact (POC). If the affected host *is not the property of the Red Team's client* (i.e., it is a "jump point" owned by another organization the Red Team is currently legally authorized to exploit), report the incident to a Trusted Agent at the appropriate service CERT (US-CERT if affected host is non-DoD). In either case, report the classification of the document, or the fact that the Red Team believes the information contained in the document to be sensitive.

Release: 2019-06
NSA:08676

Doc ID: 6672264

e. (U//~~FOUO~~) Material is discovered that may indicate criminal activity or misuse of Government information systems



(U//~~FOUO~~) Figure 4.c

1) (U//~~FOUO~~) **Incident:** Material is found that may indicate criminal or other prohibited activity (e.g., pornography on Government systems). Alternatively, the client notifies the Red Team that they have found evidence of criminal activity near where the Red Team is operating.

2) (U//~~FOUO~~) **General Instructions:** *Do not contact law enforcement*. Only AGC(IA) is authorized to contact law enforcement agencies outside of NSA.

3) (U//~~FOUO~~) **Action: Operator** – Cease all activity and immediately report the incident to the Team Lead for further guidance.

Release: 2019-06
NSA:08677

Doc ID: 6672264

Operations- log activity in [redacted] Items to be reported are the affected IP address, the account in use (including its IP address), the time of occurrence (Zulu), all operations (probing or attacking) conducted against the affected IP address, and the script file or files which document the activity.

4) (U//~~FOUO~~) **Action: Team Lead** – **Immediately** Alert Red Team branch and division leadership.

- If the incident presents an immediate risk to life, property, or national security, **immediately** contact the NSOC (NSA/CSS Security Operations Center) and/or NTOC (NSA/CSS Threat Operations Center) watch officers as directed by Red Team leadership. AGC(IA) shall also be **immediately** contacted through the aliases: DL nsocsoo and DL SOCC.

[redacted] (b)(3)-P.L. 86-36

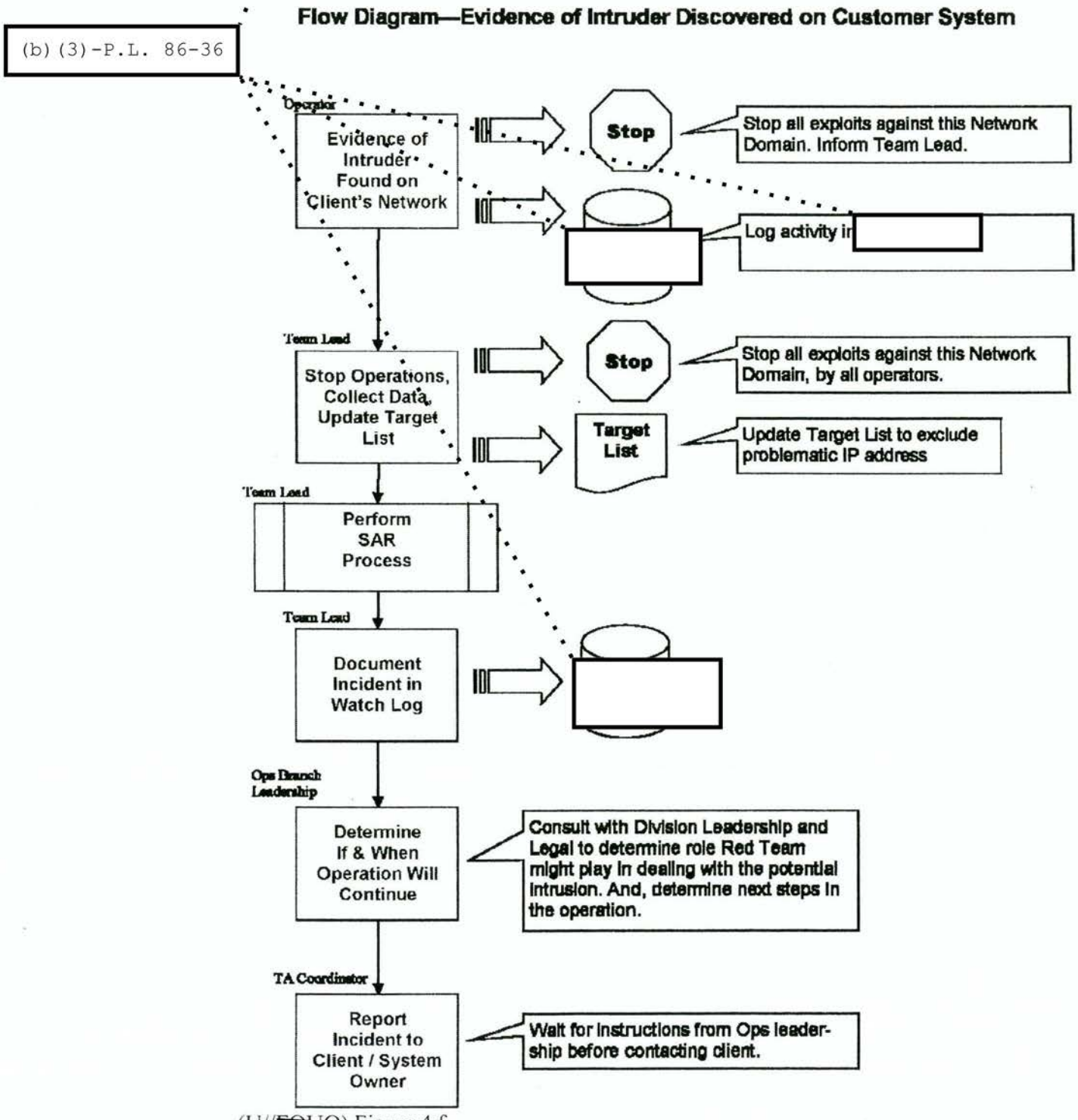
5) (U//~~FOUO~~) Generate a Significant Activity Report (SAR) and forward to the Red Team USCYBERCOM integree. If the material was found on a NSA system, also forward the SAR to NISIRT. If the material was found on a non-DoD system, forward the SAR to the US-CERT. A written report of the incident is required, and must be routed through Red Team branch and division leadership. Operations- Ensure that all activities against the affected IP address have ceased and are not resumed. Document all details provided by the operator into [redacted] under the Daily Watch Log.

Release: 2019-06
NSA:08678

IA Serial No: [redacted]-011-10 Dated: 14 June 2010

f. (U//~~FOUO~~) Evidence of an unauthorized intruder is discovered on customer networks

(b)(3)-P.L. 86-36



(U//~~FOUO~~) Figure 4.f

Release: 2019-06
NSA:08679

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

(b)(3)-P.L. 86-36

1) (U//~~FOUO~~) **Incident:** During a Red Team operation, evidence is found that may indicate an unauthorized intruder has compromised the client's network. Alternatively, the client, a Trusted Agent, NSOC, or a CERT notifies the Red Team that it has found evidence of intrusion activity near where the Red Team is operating, or publishes such evidence in an incident report.

2) (U//~~FOUO~~) **General Instructions:** *Do not contact law enforcement*. Only AGC(IA) is authorized to contact law enforcement agencies outside NSA.

3) (U//~~FOUO~~) **Action: Operator** – Cease all operations against the affected *network domain*. Immediately report the incident to the Team Lead for further guidance and log activity in [redacted] Items to be reported are the affected IP address or network domain, the account in use (including its IP address), the time of occurrence (Zulu), all operations (probing or attacking) conducted against the affected address or domain, and the script file or files which document the activity.

4) (U//~~FOUO~~) **Action: Team Lead** – Ensure that all operations against the affected network domain have ceased and will not be resumed. Document all details provided by the operator into [redacted] under the Daily Watch Log, and generate a Significant Activity Report (SAR). Ensure that scripts of all Red Team activity, as well as sniffer logs from the client's network, are maintained so that intruder activity can be differentiated from that of the Red Team. Coordinate with Red Team branch and division leadership to determine the subsequent course of action. [redacted] management, with the advice of AGC(IA), shall determine whether operations against the affected host may be resumed, whether [redacted] resources will be directed to assist in locating the intruder, or whether the current operation will be put on hold or cancelled.

5) (U//~~FOUO~~) **Action: Branch Leadership** – Coordinate with division management and AGC(IA) to determine course forward, including whether or not to notify NTOC and/or JTF-GNO if on a DoD system (or US-CERT if on a non-DoD system).

6) (U//~~FOUO~~) **Action: TA Coordinator** – When directed by Red Team Operations leadership, notify the appropriate Point of Contact (POC) for the affected host. If the affected host *is the property of the Red Team's client*, report the incident to the client's POC. If the affected host *is not the property of the Red Team's client* (i.e., it is a "jump point" owned by another organization the Red Team is legally authorized to attack), report the incident to a Trusted Agent at the appropriate service CERT. In either case, report all relevant information, including the fact

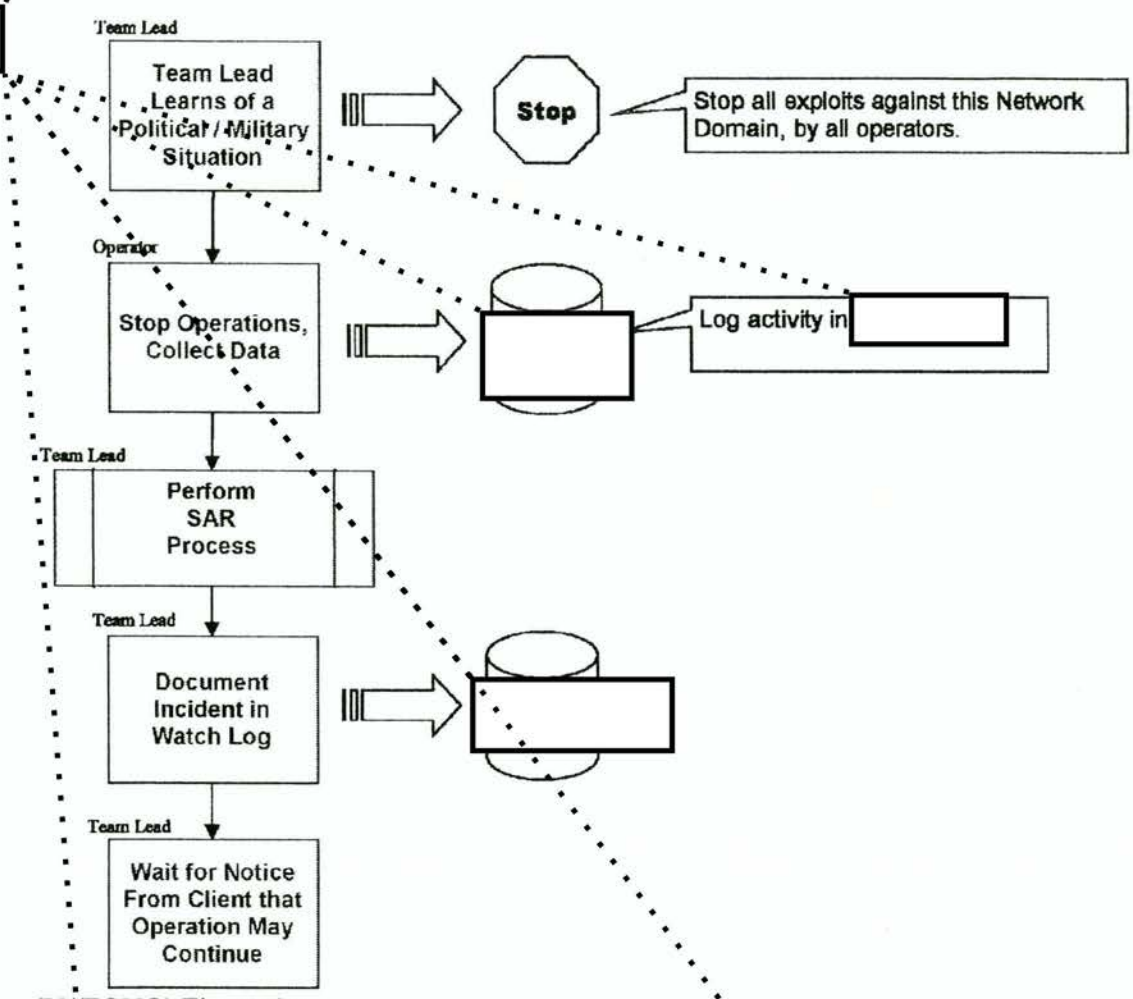
Release: 2019-06
NSA:08680

that the NSA Red Team is present on the affected systems and can coordinate tool removal if necessary.

g. (U//~~FOUO~~) A military or political situation arises that may impact Red Team operations

Flow Diagram—Military or Political Situation Arises That May Impact Operations

(b) (3)-P.L. 86-36



(U//~~FOUO~~) Figure 4.g

1) (U//~~FOUO~~) **Incident:** During the course of an exercise or assessment, the client becomes involved in real-world military or political situation that requires halting Red Team operations.

2) (U//~~FOUO~~) **Action: Operator** - Follow the Team Leader's directions. Save all scripts and work completed to this point in

3) (U//~~FOUO~~) **Action: Team Lead** - Cease all Red Team activity against the client's IP ranges or specified Commands until further notice.

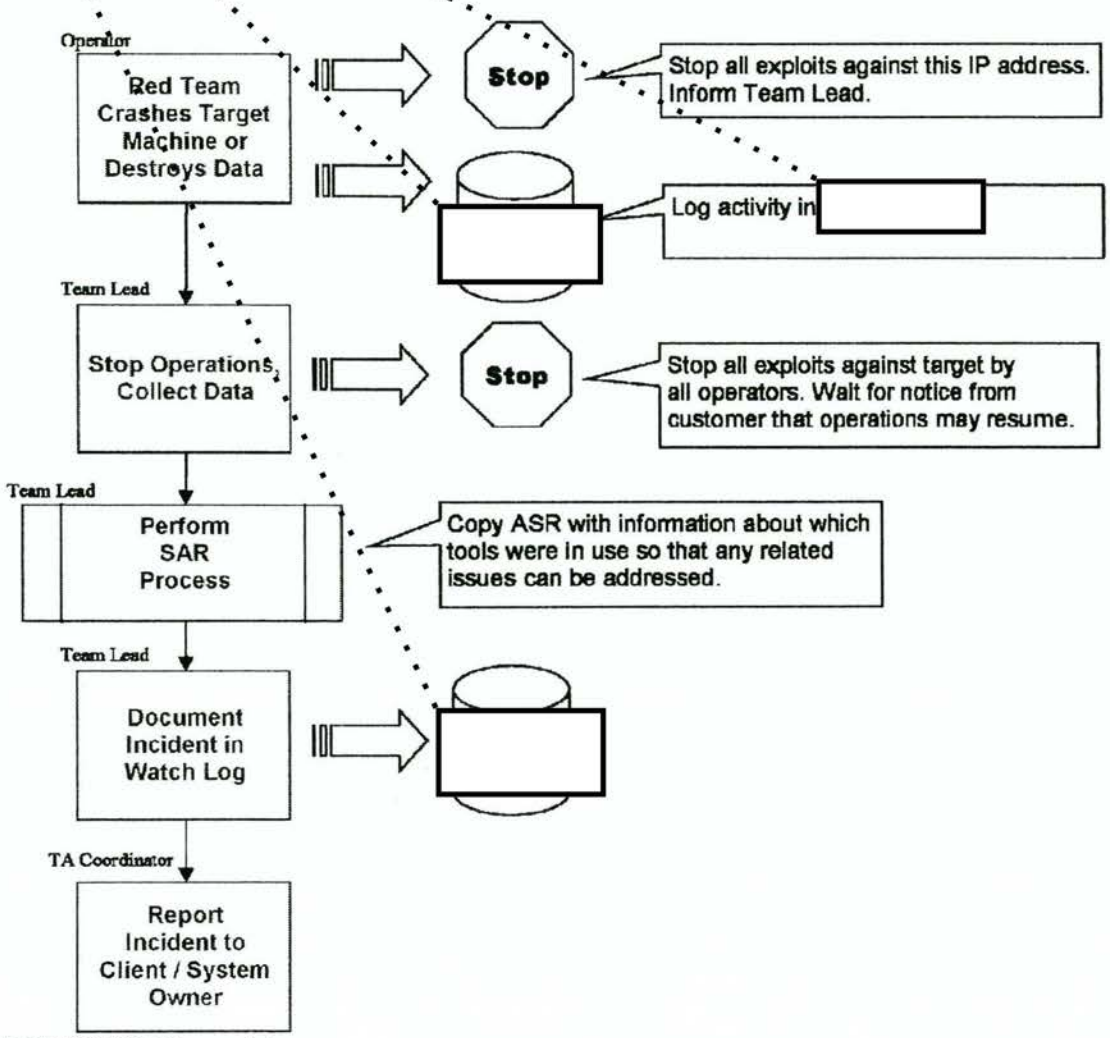
Release: 2019-06
NSA:08681

Log all pertinent information into [redacted] generate a SAR, and notify Red Team branch and division leadership. [redacted] management will determine whether Red Team operations will be put on hold or cancelled entirely. Active operations will resume only when the customer has communicated to the Red Team that operations may recommence.

(b)(3)-P.L. 86-36

h. (U//~~FOUO~~) Red Team inadvertently crashes target machine or destroys customer data

Flow Diagram—Red Team Crashes Target Machine or Destroys Customer Data



(U//~~FOUO~~) Figure 4.h

1) (U//~~FOUO~~) **Incident:** Red Team operations inadvertently crash a target machine, result in loss or destruction of data, or otherwise have an unintended negative impact on customer or third party systems.

Release: 2019-06
NSA:08682

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

2) (U//~~FOUO~~) **Action: Operator** - Immediately cease all operations against the target host. Save all scripts from that session in [redacted] and inform the Team Lead. Items to be reported are the affected IP address, the account in use (including its IP address), the time of occurrence (Zulu), all operations (probing or exploiting) conducted against the affected IP address, and the script file or files which document the activity. Take no further actions against that host unless directed by the Team Lead.

3) (U//~~FOUO~~) **Action: Team Lead** - Log all pertinent information into [redacted] Watch Log, and ensure that all relevant scripts are saved for later analysis. Generate a SAR. Notify the client as soon as possible. Alert ASR leadership, identifying any tools that may have been involved in the incident. If recommended by ASR, attempt to remove tools from exploited host. Wait for approval from client before resuming operations.

[redacted] (b) (3)-P.L. 86-36

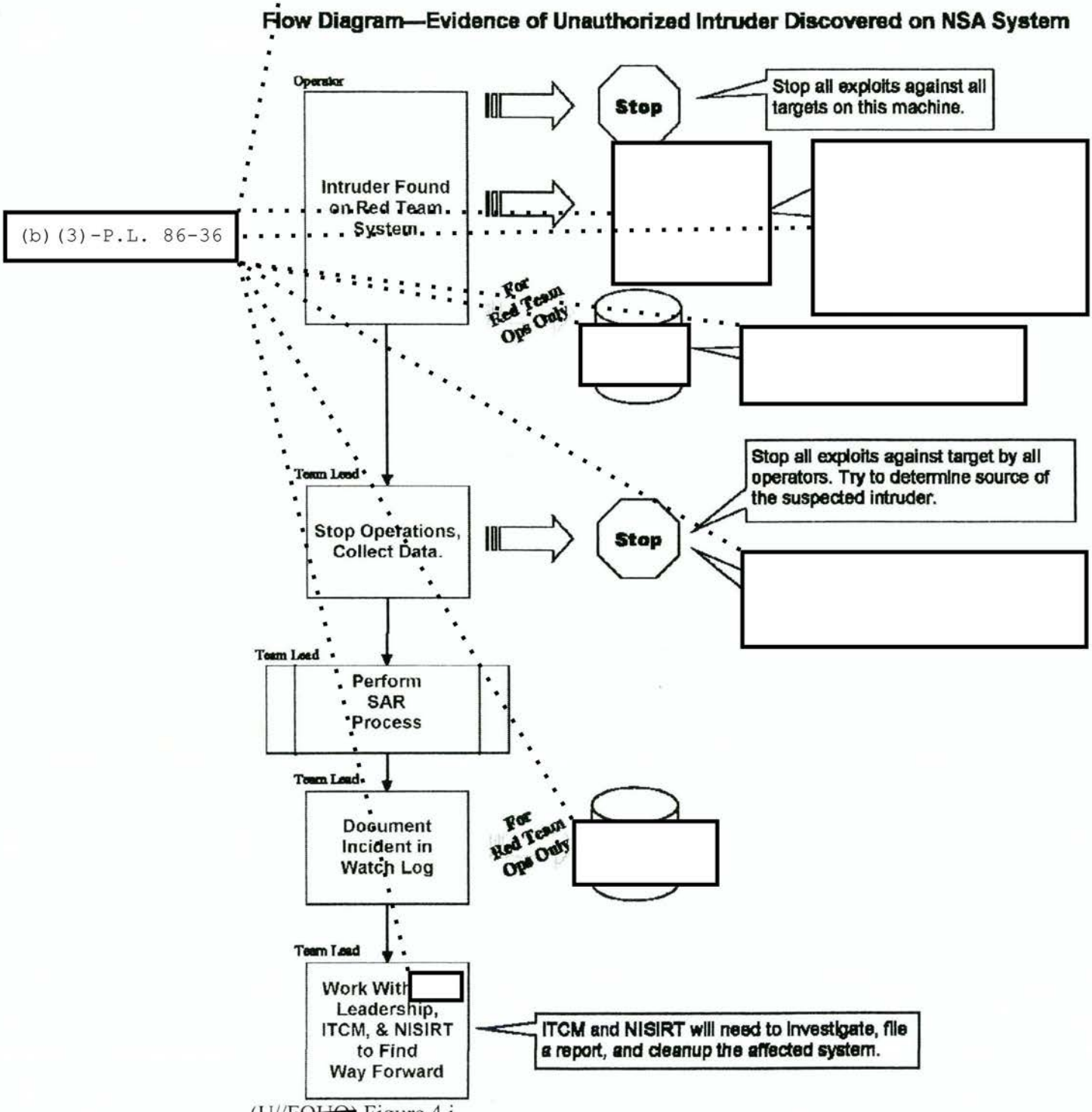
4) (U//~~FOUO~~) **Action: TA Coordinator** – Notify the client's TA and the TA of the organization with the affected target machine of the incident.

5) (U//~~FOUO~~) **Action: TA Coordinator** – If the affected host *is the property of the Red Team's client*, report the incident to the client's Trusted Agent. If the affected host *is not the property of the Red Team's client* (i.e., it is a "jump point" owned by another organization the Red Team is legally authorized to attack), report the incident to a Trusted Agent at the appropriate CERT.

6) (U//~~FOUO~~) [redacted] Oversight & Compliance shall review all incidents to help Red Team leadership determine if the events should be treated as "Items of Significant Interest to Senior Leadership" as defined in Annex D of MD-20 (see Section 5 of this document).

Release: 2019-06
NSA:08683

i. (U//~~FOUO~~) Evidence of an unauthorized intruder is discovered on Red Team systems



(U//~~FOUO~~) Figure 4.i

Release: 2019-06
NSA:08684

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

1) (U//~~FOUO~~) **Incident:** During Red Team operations, suspicious activity or files are identified on the Red Team networks. The activity may include the actual exploit and compromise of a Red Team system.

2) (U//~~FOUO~~) **Action: Operator** - Immediately inform the Team Lead and ITCM about the suspicious activity. Disconnect the network cable from the machine and save all specifics from the network monitor to a file for future reference. From another connection, identify the owner of the source IP address via a commercial DNS resolution utility, and inform the Team Lead of its ownership. *Red Team members* [redacted] ***nor shall they*** *engage in any activities outside the normal scope of Red Team authorities.*

(b)(3)-P.L. 86-36

3) (U//~~FOUO~~) **Action: Team Lead** – Ensure that the suspicious connection has been severed. [redacted] Notify Red Team branch and division leadership of the suspicious activity and any actions taken in response to it. Review the relevant network logs and save them to a file for future reference. [redacted] *Do not attempt further investigation into the orgins of the activity!* Generate a SAR and forward it to [redacted] ITCM. Unless the activity is deconflicted and identified as benign, submit an incident report to NISIRT on NSANet ("go NISIRT"). War Rooms record all relevant information in [redacted]

4) (U//~~FOUO~~) **Action: All** – If it is determined that compromise of a Red Team system has taken place, coordinate with NISIRT and [redacted] ITCM for investigation and cleanup. *Forensic imaging should only be done at the direction of ITCM and NISIRT.*

(U) OVERSIGHT AND COMPLIANCE

5. (U//~~FOUO~~) [redacted] Oversight & Compliance (O&C) shall review all SARs for potential reporting requirements as outlined in MD 20 Annex D (that document includes incident triggers not covered in this SOP). As required [redacted] O&C shall forwarding incident response reports to IV and/or IG using the form in Appendix B, and shall submit all reportable entries for the E.O. 12333 Quarterly Compliance Report (aka IG Quarterly Report). In addition to steps outlined in section 4 above, [redacted] O&C shall investigate all incidents, through spot checks or audits, to ensure the following:

Release: 2019-06
NSA:08685

Doc ID: 6672264

a. (U//~~FOUO~~) Initial reporting is done in compliance with documented procedures.

b. (U//~~FOUO~~) Containment is done in a timely and effective manner to prevent or minimize any impact to U.S. Person (USP) privacy.

c. (U//~~FOUO~~) A full understanding of the impact to USP privacy and root causes.

d. (U//~~FOUO~~) Notification of the proper entities.

(b) (3)-P.L. 86-36

e. (U//~~FOUO~~) Closure of incidents, with appropriate corrective and preventive actions.

f. (U//~~FOUO~~) Review of incidents with management, and on the E.O. 12333 Quarterly Compliance Report (aka IG Quarterly Report), as required.

6. (U//~~FOUO~~) Through regular spot checks and audits, [redacted] O&C shall monitor training, compliance, and management oversight of this SOP.

(U) REFERENCES

7. (U) References:

a. (U//~~FOUO~~) *Deconfliction* SOP, [redacted]007-2010, revised 30APR10

b. (U//~~FOUO~~) [redacted] SOP, [redacted]xxx-2010, revised xx-xxx-xx

c. (U//~~FOUO~~) IAD MANAGEMENT DIRECTIVE NO. 20 (MD-20), "IAD Oversight and Compliance Program", dated 31 May 2005, revised 16 February 2010.

d. (U//~~FOUO~~) NSA/CSS MISSION COMPLIANCE INCIDENT HANDLING GUIDE, dated 4 December 2009.

Release: 2019-06
NSA:08686

IA Serial No: [redacted]-011-10 Dated: 14 June 2010

Appendix A

(b)(3)-P.L. 86-36

Sample SAR E-Mail:

From: John Doe, Team Lead
Sent: Day, Month ##, #### ##:## PM
To: d[redacted]ar
Cc:
Subject: SAR FOR OPERATION XYZ - CEASE AND DESIST ORDER

Classification: UNCLASSIFIED//[redacted]

At the request of the client's CIO, Red Team has ceased all operations against Target until further notice due to possible real world activity. The Customer Rep will notify us when we can resume operations.

Team Lead Doe

Classification: UNCLASSIFIED//[redacted]

Release: 2019-06
NSA:08687

Doc ID: 6672264

IA Serial No. [redacted]-011-10 Dated: 14 June 2010

[redacted]
(b)(3)-P.L. 86-36

Appendix B

(U) Incident / Violation Report	(U) Response
(U//~~FOUO~~) POC, organization, phone number.	
(U//~~FOUO~~) What kind of incident is it?	
(U//~~FOUO~~) Which authority or procedures were violated? USSID SP0018, FISC Order, PAA 2007, FAA 2008, etc. (Include Court Order number, PAA or FAA Certification if applicable.)	
(U//~~FOUO~~) Which organization was responsible for the incident?	
(U//~~FOUO~~) On what date was the incident discovered?	
(U//~~FOUO~~) Which organization discovered the incident?	
(U//~~FOUO~~) How was the incident discovered?	
(U//~~FOUO~~) What are the details of the incident (in chronological order)? Things to think about when compiling your chronology. • Dates on which raw traffic, transcripts, translations, reports, etc. were destroyed at all locations, including personal files. • Did you re-issue reporting with identities masked? • Did you seek a waiver or other authority, if appropriate? On what date? Was it approved? • Did you detask a selector or stop collection? On what date? Who detasked or stopped it? • Did someone verify that the detasking occurred? If so, on what date? • Did you advise customers to	

Release: 2019-06
NSA:08688

IA Serial No. [redacted]-011-10 (b)(3)-P.L. 86-36 Dated: 14 June 2010

destroy copies, notes, etc.? On what date? Who advised them to destroy the data? Was the destruction confirmed? On what date?	
(U//~~FOUO~~) Why did the incident happen?	
(U//~~FOUO~~) How long had the incident been going on? (Be specific; put exact dates.)	
(U//~~FOUO~~) What was the volume of data collected, if any? (If no data was collected, say so.)	
(U//~~FOUO~~) What measures have you taken to mitigate the incident? *Note: You can name the U.S. person or entity when reporting a USSID SP0018 violation.*	
(U//~~FOUO~~) What measures have you taken to ensure the incident will not recur (training, counseling, internal controls review, process adjustment, SOP change, etc.)?	

REMEMBER:

- **SUBMIT TO NSA VIA REPORTING ALIAS DL IG INCIDENT REPORTS,** WITH A COPY TO DL SID IG QUARTERLY OR IAD AS APPROPRIATE.

Release: 2019-06
NSA:08689

APPENDIX F

(U//~~FOUO~~) Red Team Supplemental Rules of Engagement and Objectives for [redacted]

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

Release: 2019-06
NSA:08690

Doc ID: 6672264

(6)

~~SECRET~~

National Security Agency
Red Team

Supplemental Rules of Engagement and Objectives For

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

NATIONAL SECURITY AGENCY

"If we win, WE lose!"

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~Source Marked X1~~

~~SECRET~~

Release: 2019-06
NSA:08691

Doc ID: 6672264

~~SECRET~~

SUBJECT: (U) CNO GROUND RULES FOR NSA VAO RED TEAM DURING [redacted] Assessment

References:

A. (U) NSA VAO Red Team "Standing Rules of Engagement," 16 July 2009
B. ~~(S)~~ [redacted] Program Plan, 1 June 2009
C. (U) NSA Red Team "Supplemental Rules of Engagement and Objectives for [redacted]" 10 November 2009

1. (U) PURPOSE

(U) This document outlines the Ground Rules and Client objectives that the National Security Agency (NSA) Red Team will attempt to fulfill during this operation in accordance with references (a) and (b).

2. (U) BACKGROUND

a. (U//~~FOUO~~) Within this document the term 'Client' refers to the [redacted] and all Designated Approval Authorities (DAA) of networks the NSA Red Team will be evaluating during this operation.
b. (U//~~FOUO~~) The Client understands that by signing this document it is acknowledging receipt of and agreeing to the terms by which NSA Red Team will operate as outlined in reference (a).

~~3. (S)~~ ASSESSMENT FOCUS

a. (U//~~FOUO~~) The NSA Red Team will provide Computer Network Operations (CNO) and Open Source Research (OSR) support to [redacted] in support of [redacted] assessment.
b. (U//~~FOUO~~) The NSA Red Team will commence [redacted] operations no earlier than the signing of this document by all signatories. NSA Red Team will conclude support for this assessement no later than [redacted]
c. (U//~~FOUO~~) The primary targets are as follows:
   1) ~~(S)~~ [redacted]
   2) ~~(S)~~ [redacted]

4. (U//~~FOUO~~) [redacted] TRAINING OBJECTIVES

a. ~~(S)~~ Assist [redacted] in identifying and promoting security, stability and prosperity of the [redacted]

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~SECRET~~

Release: 2019-06
NSA:08692

~~SECRET~~

TB b. ~~(S)~~ Assist [redacted] in identifying [redacted] and identifying associated vulnerabilities.

c. ~~(S)~~ Identify [redacted]

TB d. ~~(S)~~ Specifically, the [redacted] with NSA Red Team [redacted]

1) Focus the assessment on [redacted]

2) Re-evaluate corrective measures developed by [redacted] for mitigating vulnerabilities identified in previously conducted NSA Red Team assessments [redacted]

3) Identify and template routine activities that may allow an adversary to target U.S. assets and personnel, to include:

[redacted]

(b)(1)
(b)(3)-P.L. 86-36

4) Identify vulnerabilities at facilities [redacted]

5) Identify [redacted]

a) Identify vulnerabilities in the procedures and implementation methodologies [redacted]

b) Develop specific courses of action (COA) [redacted]

- [redacted]

~~SECRET~~

Release: 2019-06
NSA:08693

6) Develop COAs and be prepared to conduct "walkthrough" demonstrations.

NOTE:

7) Identify potential mitigation techniques that could reduce vulnerabilities.

8) Identify potential locations for future NSA Red Team operations.

5. (U) NSA RED TEAM OBJECTIVES

a. ~~(S//REL)~~ Re-evaluate corrective measures developed by for mitigating vulnerabilities identified in previously conducted NSA Red Team assessments to include but not limited to:

(b)(1)
(b)(3)-P.L. 86-36

b. ~~(S//REL)~~

c. ~~(S//REL)~~

d. ~~(S//REL)~~

e. ~~(S//REL)~~ Enhance OPSEC awareness,

f. ~~(S//REL)~~ Illustrate the OPSEC implications of

g. ~~(S//REL)~~

h. ~~(S//REL)~~ Establish and maintain

Release: 2019-06
NSA:08694

(b) (1)
(b) (3)-P.L. 86-36

~~SECRET~~

i. ~~(S//REL)~~ Identify and exploit weaknesses

j. ~~(S//REL)~~ Use data collected

6. (U) **RED TEAM NEGOTIABLE SERVICES**

a. (U//~~FOUO~~) The Client requests that Red Team may use is the (pending NSA General Counsel review and approval).

b. ~~(S)~~ The Client requests

c. (U//~~FOUO~~) The Client requests NSA Red Team personnel After Action Report (AAR) and associated briefs.

d. ~~(S)~~ The NSA Red Team

e. (U//~~FOUO~~) The NSA Red Team will provide both an AAB and an AAR to the Client no later than 30 days after the conclusion of this operation.

f. (U//~~FOUO~~) The Client agrees to a NSA Staff Assist Visit (SAV) approximately 60 days after the completion of this operation. This SAV is intended to provide the Client with in-depth technical assistance on critical items and suggested remediation actions to be implemented.

7. (U) Reference (c) is cancelled.

(b) (3)-P.L. 86-36

The undersigned have reviewed the Ground Rules for NSA Red Team support of and concur as written.

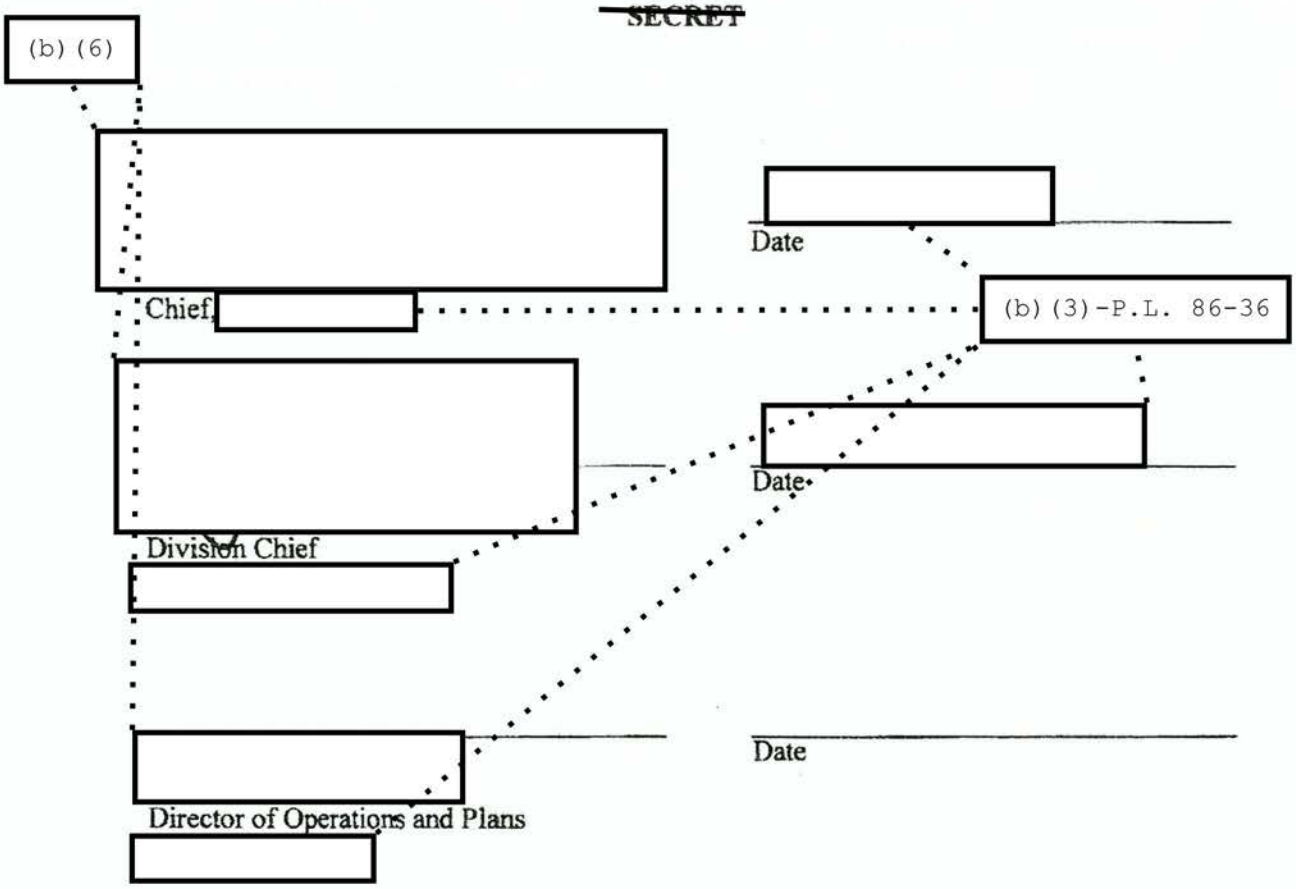
Date

National Security Agency

~~SECRET~~

(b) (3)-P.L. 86-36
(b) (6)

Release: 2019-06
NSA:08695



Release: 2019-06
NSA:08696

Doc ID: 6672264

APPENDIX G

(U) Classification Review of Red Team Analyst Report

Release: 2019-06
NSA:08697

~~SECRET//NOFORN~~

(b)(3)-P.L. 86-36

5 April 2013

Memorandum

To: D14

From:

Subject: Classification Review

(b)(1)
(b)(3)-P.L. 86-36

~~(S//NF)~~ I have reviewed the provided documents and determined that all portions are currently and properly classified SECRET//NOFORN.

~~(S//NF)~~ On 3 April 2013, I consulted with Neal Ziring, IA Technical Director to discuss IA equities. The NSA Red Team Classification Guide, dated 12 October 2011, authorizes information in Red Team reports containing risk information relating to technical/exploit information to be classified SECRET at a minimum. Given that all of the information in the documents falls into this category, all portions qualify for SECRET-level protection under this classification guide.

~~(S//NF)~~ On 3 April 2013, I also met with from to discuss the classification of the equities in the documents information classified at the SECRET//NOFORN level includes:

-
-
-

had particular concerns with the details

(b)(1)

(b)(6)

~~(S//NF)~~ Other DoD information that likely would have been classified SECRET at the time,

(U//~~FOUO~~) Because the equities outlined above fall under multiple and overlapping authorities, all information in the documents remains currently and properly classified SECRET//NOFORN.

(b)(3)-P.L. 86-36

Classified By:
Derived From: Multiple Sources, NSA/CSSM 1-52 dated 20070108
Declassify On: ~~20361231~~

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08698

(b)(3)-P.L. 86-36

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Classification: ~~SECRET//NOFORN~~

Release: 2019-06
NSA:08699

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08700

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08701

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08702

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08703

~~SECRET//NOFORN~~

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

~~SECRET//NOFORN~~

Release: 2019-06
NSA:08704

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08705

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08706

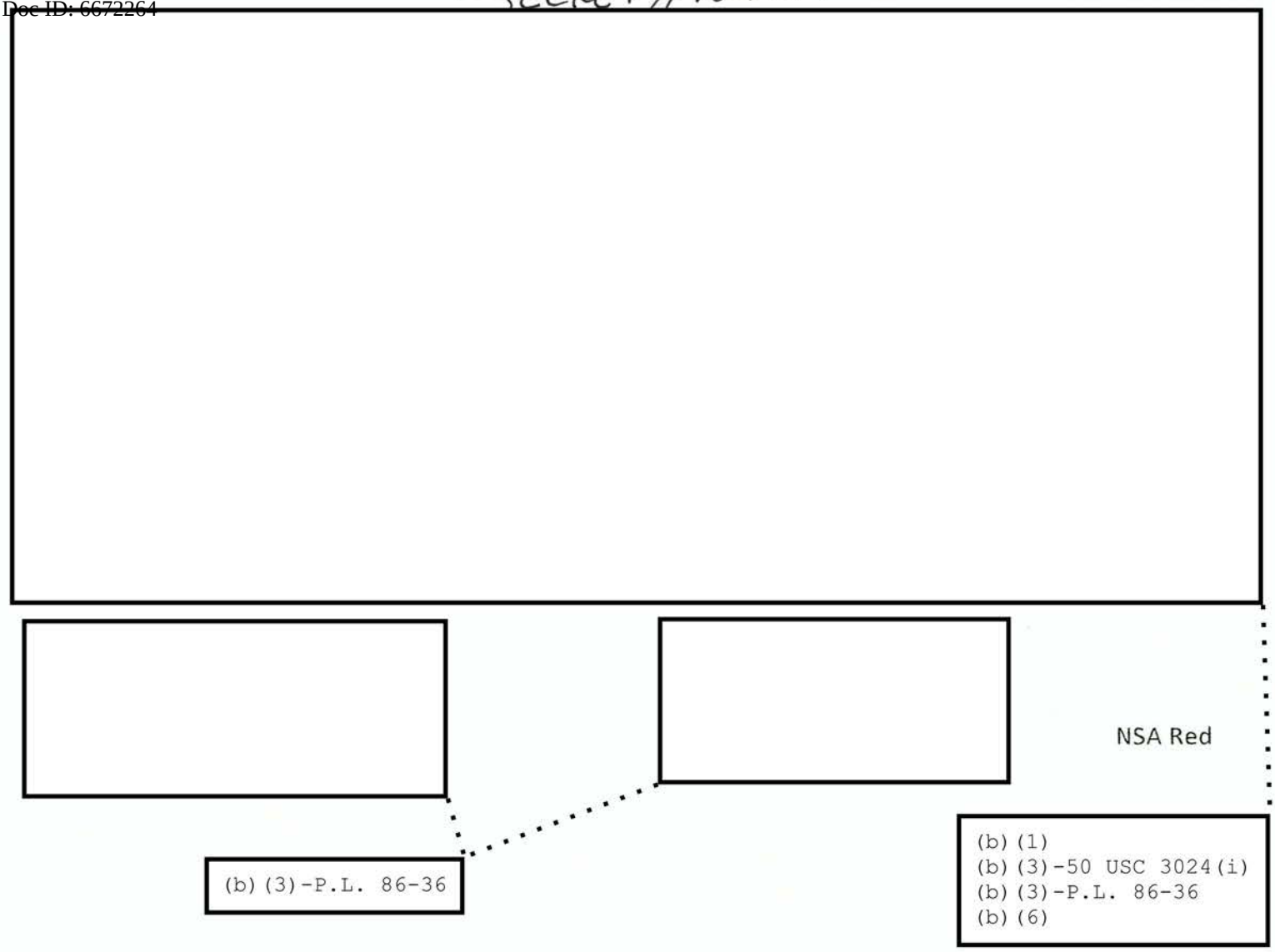
(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08707

Doc ID: 6672264

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
(b)(6)

Release: 2019-06
NSA:08708



Release: 2019-06
NSA:08709

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

(U) NSA/CSS CLASSIFICATION GUIDE TITLE/NUMBER: NSA Red Team, 3-13

(U) PUBLICATION DATE: 12 October 2011

(U//~~FOUO~~) OFFICE OF ORIGIN: IAD Remote and Deployed Operations, [redacted]

(U//~~FOUO~~) POC: [redacted] IAD Current Operations, [redacted] 968-5674 (NSTS)

(U) ORIGINAL CLASSIFICATION AUTHORITY: Debora A. Plunkett, Information Assurance Director

(b)(3)-P.L. 86-36

(U) This guide provides specific classification guidance pertaining to NSA Red Team activities (tools, techniques, procedures, results). NSA Red Team activities are intended to demonstrate (notionally or during an exercise) the potential impact of computer network vulnerabilities and weaknesses on the operational readiness, effectiveness, and response of a U.S. Military Command, other U.S. government organization, or the U.S. in general. Upon request by a customer, NSA Red Team will emulate an adversary and conduct Computer Network Operations (CNO) on that customer's network(s) to find network vulnerabilities and weaknesses, demonstrate the impact an adversary can have on the network(s), and provide suggested mitigations for the vulnerabilities and weaknesses.

(U) For any programs involving the release of information or technology to foreign partners, please contact the Information Assurance Directorate (IAD) Operations Group [redacted] within the NSA Foreign Affairs Directorate.

Description of Information	Classification/ Markings	Reason	Declass	Remarks
A.1. (U) The fact that NSA/CSS has a Red Team.	UNCLASSIFIED	N/A	N/A	
A.2. (U) The mission of the NSA Red Team is to: • (U) Identify vulnerabilities and weaknesses in United States cyber information systems; • (U) Simulate real world CNO adversary or opposition forces during DoD and Government assessments, exercises, and Information Operations (IO) activities; • (U) Demonstrate the impact of identified vulnerabilities and weaknesses in a near real world environment; and • (U) Provide recommendations to mitigate identified vulnerabilities and weaknesses.	UNCLASSIFIED	N/A	N/A	(U) In support of the mission, Red Team develops and tests computer network exploit and attack tools, techniques, and procedures for use by Red Team.
A.3. (U) The Red Team cover term for ongoing or future operations and the dates/times that the NSA Red Team is active with no other details.	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U) Either the cover term or the dates of Red Team activity separately with no other details are UNCLASSIFIED.
A.4. (U) Information regarding ongoing or future	UNCLASSIFIED//	N/A	N/A	(U) Classification

UNCLASSIFIED/~~FOR OFFICIAL USE ONLY~~

Red Team operations that includes the system or the customer, and other amplifying information such as the: • (U) Target organization; • (U) Red Team cover term; and/or • (U) Dates/times that the NSA Red Team is active.	FOR OFFICIAL USE ONLY At a minimum			and releasability depends on the sensitivity of the system and/or customer.
A.5. (U) The approximate number of personnel in the NSA Red Team (total or any subsets).	UNCLASSIFIED	N/A	N/A	(U) The Red Team will occasionally need to provide the approximate number of individuals who will be devoted to a customer's activity. The exact number of personnel in the NSA Red Team (total or any subsets) is classified CONFIDENTIAL// REL TO USA, FVEY.
B. (U) Red Team tools:				
B.1. (U) Information that could be used to identify Red Team activity.	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	(U) An example is a description of network traffic that can be used as a signature to identify Red Team activity.
B.2. (U) Information that could be used to disrupt Red Team activity.	UNCLASSIFIED// FOR OFFICIAL USE ONLY At a minimum	N/A	N/A	(U) Classification is dependent on the details about the customer, target, and potential adversary.
B.3. (U) Red Team non-exploit tool (source code, documentation or executable) that does not target or contain information about vulnerabilities, and that performs a function that is known in the unclassified community.	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	
B.4. (U) Red Team exploit tool containing only publicly known technical/exploit information for publicly known vulnerabilities for commercial off-the-shelf (COTS) systems or components (hardware, firmware, or software).	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	
B.5. (U) Red Team exploit tool containing technical/exploit information for vulnerabilities for COTS systems or components (hardware, firmware, or software) for which the vulnerability information is available within the public domain and for which there is unclassified value-added analysis by Red Team or other DoD/IC	UNCLASSIFIED// FOR OFFICIAL USE ONLY	N/A	N/A	

Release: 2019-06
NSA:08711

(b)(3)-P.L. 86-36

component.				
B.6. (U) Red Team exploit tool containing technical/exploit information for vulnerabilities for COTS systems or components (hardware, firmware, or software) for which the vulnerability information is not available within the public domain, and for which the vulnerability has **not** been approved for declassification by the NSA Issue Resolution Process (IRP) or other declassification process.				
B.7. (U) Red Team tools containing technical/exploit information for vulnerabilities for COTS systems or components (hardware, firmware, or software) for which the vulnerability information is not available within the public domain, but for which the vulnerability **has been** approved for declassification.				
C.1. (U) Information about publicly known vulnerabilities within DoD or other U.S. government systems observed during Red Team activities **not attributed to** a specific system or customer.	UNCLASSIFIED	N/A	N/A	

Release: 2019-06
NSA:08712

Doc ID: 6672264

(b)(3)-P.L. 86-36

(U) *Declassification in 25 years indicates that the information is classified for 25 years from the date a document is created, or 25 years from the date of this original classification decision, whichever is later.

(U) DEFINITIONS

1. (U) Computer Network Operations (CNO): Comprised of Computer Network Attack, Computer Network Defense, and related Computer Network Exploitation enabling operations. (DODD 3600.01)

2. (U) Commercial Off-the-Shelf (COTS): A component, product, or system that has been developed, produced, and distributed by a commercial enterprise, and is available on the commercial market. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

3. (U) Exploit: To perform or demonstrate the compromise or violation of one or more security services of a particular system by taking advantage of one or more specific vulnerabilities. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

4. (U) Exploit tool: A tool or technique that attempts to take advantage of or demonstrate a vulnerability or weakness, such as a misconfiguration, and which incorporates or encapsulates the technical details of the attack techniques employed.

5. (U) Government Off-the-Shelf (GOTS): A component, product, or system that has been developed, produced, and distributed by a U.S. Government entity or under U.S. Government contract, and is not available on the commercial market. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

6. (U) Information Assurance (IA): Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

7. (U) Information Operations (IO): The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. (Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition)

Release: 2019-06
NSA:08713

Doc ID: 6672264

8. (U) Publicly Known Vulnerability: A vulnerability is publicly known if there is a paper or other published documentation in the open source (e.g., that which could be found on the internet, in trade journals, etc.) which specifically discusses the vulnerability under consideration and how the vulnerability could be exploited. This does NOT include information currently and properly protected as U//FOUO or classified that has been inappropriately released to the public. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

9. (U) Red Team: An IAD Remote and Deployed Operations organization that performs red teaming (i.e., role plays hostile actors) of customer networks, exploiting the networks to find and demonstrate the impact of vulnerabilities.

10. (U) Red Team Tool: A software tool developed or modified by the Red Team for its use.

11. (U) Risk: The potential impact on a user if the vulnerability was exposed by an adversary.

12. (U) Vulnerability: A discovered weakness in a system or an IA COTS or GOTS component or product that can be exploited. (Information Assurance Vulnerabilities and Weaknesses Classification Guide, 03-02)

Release: 2019-06
NSA:08714

APPENDIX H

(U//~~FOUO~~) [redacted] response to the OIG's Tentative Conclusions

[redacted]
(b)(3)-P.L. 86-36
(b)(6)

20 MAR 2014

From:

To: Inspector for the NSA/CSS Office of the Inspector General

Subj: NSA/CSS Office of the Inspector General (OIG) Red Team Investigation

1. This statement is submitted in response to 18 March 2014 email containing the following tentative OIG conclusions:

(b) (3)-P.L. 86-36
(b) (6)

"There is one issue, that you did not follow the Red Team SOP.

The OIG is tentatively concluding that you failed to ensure that the Red Team took required actions to report and respond to incidents as required by the Red Team SOP after you were informed that an individual was involved in possible criminal activity and that this same individual inappropriately maintained and passed classified information through an unclassified computer network."

2. NSA Red Team Standard Operating Procedures (SOP) are specifically for members of the Red Team and not any person or element in the IAD chain-of-command above the Red Team Division level. As the I was not subject to Red Team SOP. I was subject, as is the case with other NSA employees, to Federal laws and the DoD and NSA/CSS policies and directives pertaining to my duties and responsibilities.

(b) (3)-P.L. 86-36

3. On or about Red Team leadership informed me that the war room team believed that who was being monitored by the Red Team under this operation, might be "involved in an affair." I requested proof of this allegation, but neither saw nor was provided any. Both Red Team leadership and the acting Chief of looked into the matter and reported that there was "nothing there." The analysts themselves indicated that there was "no evidence of a crime." Even so, although I had no legal or ethical requirement to report the unsubstantiated rumors or speculation of others, I did discuss this matter with my supervisor, the Chief a member of the Defense Intelligence Senior Executive Service. He concurred that this matter did not meet the established reporting criteria. Had either of us believed there was any evidence of a crime, especially a "significant crime," as specified in NSA/CSS policy, we would have notified IAD lawyers immediately.

4. All NSA/CSS personnel are required to report violations of Federal criminal law to the Office of General Counsel. Independent of the guidance and oversight provided to the Red Team through their chain-of-command, the Red Team leadership and operators met routinely with IAD lawyers to discuss legal issues pertaining to operations and operational guidance. They normally met once a week. IAD lawyers and IAD Oversight and Compliance personnel attended and actively participated in the weekly operational briefing. If anybody on Red Team had any legal concern about this incident, they could have and should have raised it with the two IAD lawyers with whom they routinely

(b) (1)
(b) (3)-P.L. 86-36

Release: 2019-06
NSA:08716

(b) (1)
(b) (3)-P.L. 86-36

met. In fact, if they had any evidence of a significant crime, they had an obligation to do so. They did not bring this issue up with the lawyers.

5. [redacted] was conducted in support of another DoD agency. The Red Team met routinely with representatives of this agency, sometimes as much as every two weeks. The Red Team did not discuss this matter of the alleged extramarital affair with representatives of this agency.

6. [redacted] I was the [redacted] The Chief was TDY. I mentioned to the next person present in my chain-of-command, the Deputy Chief of [redacted] that the Red Team's [redacted] analysts had speculated [redacted] without supporting evidence, [redacted] might have been involved in an affair. He reported this up the IAD chain-of-command and, to my knowledge, this is what triggered the NSA/CSS OIG investigation.

(b) (6)
(b) (3)-P.L. 86-36

7. Red Team discovers, exploits and mitigates U.S. Government computer network vulnerabilities; it does not monitor someone's personal matters. NSA Information Assurance policy, referenced in Red Team SOP, states that matters of a personal nature are off-limits. [redacted] analysts arrived at their speculation concerning an extramarital affair by [redacted] and Chief/Deputy Chief of Red Team to ensure that the Red Team was operating in accordance with its own SOP and [redacted] ground rules. As part of this review, they put measures in place to ensure leadership would be aware of when Red Team operators were targeting the U.S. government computer systems and communications [redacted] for the authorized purposes of network vulnerability discovery, exploitation and mitigation. Red Team members were directed to re-familiarize themselves with Red Team SOP and the specific ground rules for their particular operation. Due to the actions taken, no violations of policy or law took place.

8. Nobody ever informed me that [redacted] had "...inappropriately maintained and passed classified information through an unclassified computer network." An OIG email of 14 March 2014 is the first time this issue was brought to my attention. Red Team, as well as [redacted] and other IAD operational elements, routinely found classified information on unclassified systems during their operations and took appropriate action in accordance with SOP. I know of no instance where this was not the case.

9. On the advice of counsel, on 19 March 2014 I submitted a FOIA request to NSA for the Red Team investigation. I cannot fully or adequately respond to its findings if I have not been shown the actual investigative report. If the report can be provided, I would request that I be allowed to provide any additional comments, as appropriate, after I am able to review it.

(b) (3)-P.L. 86-36
(b) (6)

[redacted]

Release: 2019-06
NSA:08717