(U) Cryptologic Intelligence Oversight Implementation Plan

Prepared by:

USCYBERCOM/J2

POC: [redacted]

13 June 2013

(U) Reviewed by:

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~)

(U//~~FOUO~~)

(b)(3) 10 U.S.C. §130b

(b)(6)

(U) CIO Plan Approved by:

(U//~~FOUO~~) [redacted]

(U//~~FOUO~~)

Classified By: [redacted]

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On: 20380501

(U) Table of Contents

(U) Purpose:

(U) The purpose of this Implementation Plan is to outline the roles and responsibilities of the United States Cyber Command (USCYBERCOM) Cryptologic Intelligence Oversight (CIO) program. This CIO Plan ties intelligence oversight measures, resulting from USCYBERCOM's SIGINT authority, mission, and access, as well as its Defensive Cyber Operations mission and access, together, and will serve as the foundational document for USCYBERCOM's Oversight and Compliance (O&C) program. This plan is aimed at developing a compliance construct to support intelligence oversight of National Security Agency/Central Security Service (NSA/CSS) mission activities delegated to USCYBERCOM and access to NSA/CSS data provided to USCYBERCOM, which, as needed, may include activities and data obtained pursuant to the Foreign Intelligence Surveillance Act (FISA) as amended by the FISA Amendments Act (FAA). Specific decisions regarding mission delegations and sharing of NSA/CSS data will be documented separately.

(U) Moreover, the plan will ensure that the missions conducted by USCYBERCOM and subordinate forces are performed in accordance with NSA/CSS directives, regulations, procedures, and policies, and that the risks associated with access to unevaluated and unminimized SIGINT and NSA Information Assurance (IA) data are fully understood and compliance measures are defined and implemented to mitigate these risks at each location.

(U//~~FOUO~~) This plan will not supersede reporting procedures prescribed for service components assigned duties under extant United States Signal Intelligence Directives (USSID). As such, Service Cyber Components (hereafter identified as SC) should deconflict and coordinate mandatory intelligence oversight reporting prescribed in governing USSIDs with cyber counterparts addressed in this implementation plan.

(U) This plan will be implemented while the command and control constructs for the Cyber National Mission Force (CNMF) and Cyber Combat Mission Force (CCMF) are developed. Once the supporting elements governed by those constructs establish robust O&C programs (no sooner than FY2014), applicable annexes to command intelligence oversight program instructions should be written.

(U) Program Description:

(U//~~FOUO~~) In November 2012, the Director of the National Security Agency (DIRNSA) agreed to delegate SIGINT authorities to specified USCYBERCOM staff personnel and USCYBERCOM-directed Service cyber forces to conduct SIGINT activities in support of planning and execution of approved cyberspace operations and mission needs. This authority will allow the direction and tasking of SIGINT Development and Computer Network Exploitation activities, and the processing, analysis, reporting, and dissemination of SIGINT information, as delegated and in accordance with NSA policies, procedures, and directives.

(~~S//REL TO USA, FVEY~~) As envisioned, specified members of the USCYBERCOM staff and USCYBERCOM-subordinated Cyber Mission Force (CMF) personnel will require access to SIGINT and NSA IA data to perform their mission duties. Access to that data requires these

cyber forces to adhere to all NSA/Central Security Service (CSS) O&C rules and regulations. As outlined in the 30 November 2011 Decision Memorandum, DIRNSA approved shifting CIO responsibilities from NSA/Signals Intelligence Directorate (SID) to USCYBERCOM. In accordance with this memorandum, USCYBERCOM and SC personnel shall adhere to the SID Oversight and Compliance (SV) standards within the NSA/CSS Signals Intelligence Directorate Oversight and Compliance Policy (USSID SP0019), as well as develop and implement a CIO program in accordance with Executive Order (E.O.) 12333, DoD 5240.1-R, USSID SP0018, USSID SP0021, NSA/CSS Policy 1-23, and the Foreign Intelligence Surveillance Act (FISA) Amendment Act (FAA).

(U//~~FOUO~~) Information Assurance Directorate (IAD) Guidance Number 350, *Guidance for IAD Information Sharing with USCYBERCOM*, prescribes the procedures and responsibilities for sharing information that was obtained or produced by IAD under its Information Assurance authority. Subject to the handling and dissemination restrictions of IAD governing policies, procedures, or regulations, the information which may be shared includes: data, access to data stores, vulnerability assessments, reports, issuances, tippers, situational awareness data, tools, capabilities, briefings and technical exchanges. When operating on NSA IA infrastructure, using NSA/CSS IA data stores, or using IAD obtained or produced information USCYBERCOM personnel and subordinate forces shall comply with IAD Management Directive (MD) Number 20, *IA Oversight and Compliance Program* standards to ensure the privacy rights of United States (U.S.) persons are safeguarded and information sharing activities comply with applicable U.S. laws, executive orders, regulations, directives, and policies.

(U) Procedures:

(U) USCYBERCOM will designate a Cryptologic Intelligence Oversight Program Manager (CIOPM) within the Intelligence Directorate (J2) to oversee the Command CIO program. This CIOPM will also oversee the CIO program for the CMF.

(U) Until the CNMF Headquarters (CNMF HQ) is fully staffed and an appropriate O&C program is established by that HQ for assigned teams (i.e., National Mission Team (NMT), National Support Team (NST)), the USCYBERCOM CIOPM will also oversee those O&C efforts. In the longer term, a CIOPM shall be designated in the CNMF HQ and a CIO program to oversee SIGINT and Defensive Cyber Operations oversight programs attendant to the CNMF mission will be established. That CIOPM will oversee all O&C efforts within the CNMF and coordinate program administration through the USCYBERCOM CIOPM.

(U) The SCs (i.e., Air Force Cyber, Army Cyber, Fleet Cyber, and Marine Force Cyber) will designate a CIOPM to oversee SIGINT oversight programs attendant to the assigned CCMF (i.e., Combat Mission Team (CMT), Combat Support Team (CST)). These CIOPMs will oversee the O&C efforts performed by subordinated CCMF and coordinate program administration through the USCYBERCOM CIOPM.

(U) As the mission develops and the nature of the command and control is discerned, a CIOPM shall be designated and an O&C program shall be established to oversee the Cyber Protection Force (CPF) mission. As with the CNMF and CCMF, this CIOPM will oversee O&C efforts for

the CPF and coordinate program administration through the USCYBERCOM CIOPM. Figure 1 below portrays the notional organizational structure.

(U) In all cases, CIOPMs shall designate and assign sufficient numbers of Cryptologic Intelligence Oversight Officers (CIOO) to manage all respective cyber programs that will access/use unevaluated and unminimized SIGINT and NSA IA data. CIOPMs shall also identify and assign sufficient numbers of auditors (at least two mission auditors per NSA/CSS content data store) to review queries made against auditable SIGINT data or repositories that support assigned missions.

(U//~~FOUO~~) Conceptually, personnel performing CIOO and auditing duties should be integrated within the teams performing SIGINT activities and Defensive Cyber Operations. Such duties require target knowledge, familiarity with the queries appropriate for the cyber mission and the attendant SIGINT production, and an understanding of the laws, directives, and policies governing SIGINT activities (e.g., USSID SP0019). Moreover, personnel performing these duties should advise and mentor team operators, analysts, and reporters regarding the legality and propriety of SIGINT activities and Defensive Cyber Operations and the protection of U.S. persons' Fourth Amendment rights IAW USSID SP0018 and IAD Mission Directive (MD) Number 20. As envisioned and recommended, CIOO and auditing duties would be performed as collateral duties, though sufficient numbers of personnel would be required to complete tasks outlined in the governing directives.

(U) CIOOs must be familiar with the data stores and types of data contained therein, and ensure that personnel requiring access are appropriately trained. NSA user based access control solutions (e.g., [redacted] will be used to verify eligibility for access to data and ensure training requirements are met. CIOOs must ensure all personnel operating with SIGINT authority understand and abide by rules governing the conduct of SIGINT activities. CIOOs must arrange and track SIGINT and NSA IA compliance training. Moreover, CIOOs must implement and assess standards to monitor mission operations and report incidents of noncompliance and take corrective actions to remediate noncompliant activity. It is considered good practice for an alternate CIOO to be trained and in place to ensure oversight responsibilities are always supported.

(U//~~FOUO~~) Auditors are responsible for reviewing all queries (including routinely scheduled queries) in specified NSA/CSS content data stores. Moreover, all queries must be audited within 24-hours of receipt, or on the next normal duty day for the auditing team (as long as no more than three business days elapse). Auditors work in teams in order to balance workloads, but all auditors are responsible for ensuring queries against auditable NSA/CSS data stores are reviewed. Since the teams associated with the CNMF and CCMF will likely stand watches when performing SIGINT activities, auditors must consider the course of action if a targeting, dissemination, or other type of incident occurs. The analyst, auditor, or CIOO may submit an incident report. The determination of who should submit an incident report depends on who is best able to provide the necessary level of detail pertaining to the incident. The auditor and CIOO should be copied on all incident reports.

(U//~~FOUO~~) Examples of reportable incidents include:

- Unintentional collection or dissemination of US Person information;
- Sharing unevaluated and unminimized SIGINT outside of the SIGINT production chain;
- Any other instance of unauthorized access to unevaluated and unminimized SIGINT or NSA IA data;
- Unauthorized collection, processing, retention, or dissemination of information that unlawfully identifies a U.S. person;
- Unintentional collection and dissemination that occurs pursuant to the FISA to include FAA;
- Any illegal, improper, or otherwise questionable activity not covered by the previous categories.

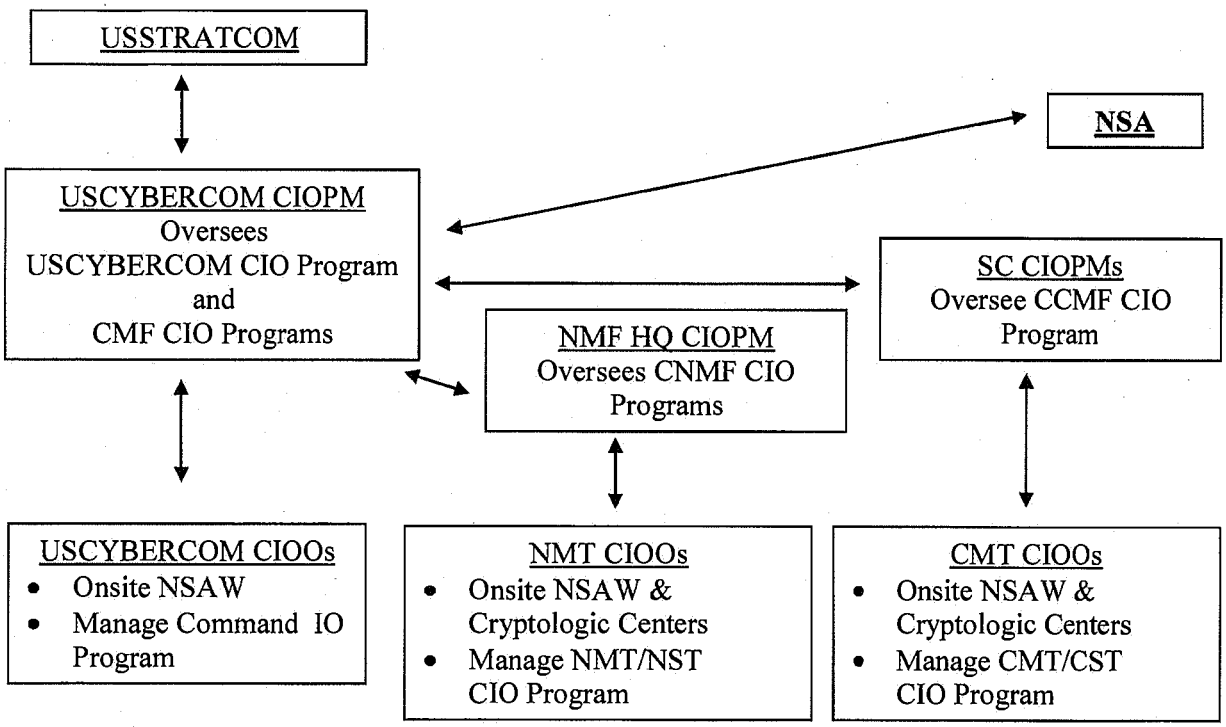

Figure1.

(U) CIOPMs will ensure:

- (U//~~FOUO~~) Fully qualified on-site CIOOs, in accordance with USSID SP0019, are identified for each CMF mission requiring access/use of SIGINT (e.g., National Mission Teams and assigned Support Teams (DST), CCMT);
- (U//~~FOUO~~) Fully qualified on-site mission compliance officers (MCOs) in accordance with IAD MD Number 20, *IA Oversight and Compliance Program*, are identified with each CMF mission to ensure compliance with NSA IA procedures when utilizing NSA/CSS provided IA resources;

- (U//~~FOUO~~) On-site CIOOs acknowledge responsibility for ensuring that incidents of non-compliance are reported immediately upon recognition to the NSA/CSS SV, IV, and Inspector General (IG), through the USCYBERCOM CIOPM, and applicable SC CIOPM;
- (U//~~FOUO~~) On-site CIOOs produce CIO Quarterly Reports and forward those reports to USCYBERCOM CIOPM through the applicable SC CIOPM, with a "cc" to NSA SV and IV;
- (U//~~FOUO~~) A sufficient number of CIOOs are assigned to perform assigned duties effectively.

(U) SC CIOOs will ensure:

- (U//~~FOUO~~) All personnel performing SIGINT activities are knowledgeable of the current rules governing SIGINT activities and have completed mandatory training courses before being granted access to SIGINT;
- (U//~~FOUO~~) All personnel comply with standards outlined in USSID SP0019, to include the physical measures detailed in Annex A;
- (U//~~FOUO~~) Compliance verification is performed in accordance with Section 4 of USSID SP0019;
- (U//~~FOUO~~) A comprehensive auditing program is established to ensure that queries made against auditable NSA/CSS data or repositories are compliant with U.S. laws and procedures that govern SIGINT activities (Section 5 of USSID SP0019 germane);
- (U//~~FOUO~~) All personnel performing USCYBERCOM Defensive Cyber Operations and accessing NSA/CSS data which contains information to/from/about a U.S. person or U.S. person's identifying information, and the conduct of penetration testing, readiness testing support, network monitoring, and communications security monitoring, are knowledgeable of the current rules governing NSA IA activities and have completed mandatory training courses;
- (U//~~FOUO~~) Compliance verification is performed in accordance with Annex C of IAD MD Number. 20.

(U) Roles and Responsibilities:

(U) USCYBERCOM will direct and guide the cryptologic intelligence oversight activities of the Command, as well as those of the CMF. Moreover, USCYBERCOM will ensure that when operating on NSA IA infrastructure, using IAD data stores, or using IAD obtained or produced information USCYBERCOM personnel and subordinate forces shall comply with IAD directives and procedures. The USCYBERCOM Intelligence Directorate (J2) will designate a CIOPM, who will oversee the implementation of the Command's CIO program and those executed by the CNMF HQ CIOPM and SC CIOPMs. All CIOPMs will implement programs that ensure SIGINT activities comply with the laws, regulations, and policies governing SIGINT protect the constitutional rights of U.S. persons. CIOPMs will direct the efforts of on-site CIOOs who will ensure that daily cryptologic activities supporting cyber operations are conducted in a manner consistent with E.O. 12333, as amended, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, USSID SP0018, and SID MD 422, as well as National Telecommunications and Information Systems Security Directive (NTISSD) 600, 18 U.S.C. Sec 2510 et seq. (Federal Wiretap Act), 18

U.S.C. Sec. 2510 note, Section 107(b) of the Electronic Communications Privacy Act of 1986 , P.L. 99.508, and procedures prescribed in IAD MD Number 20. Moreover, CIOOs will be responsible for advising local managers regarding compliance issues, risks and mitigation procedures, and promoting lawful conduct of cryptologic activities at their respective commands in accordance with SID MD 422 and IAD MD Number 20.

(U) Training:

(U) All USCYBERCOM, SC, and CMF personnel with access to unevaluated and unminimized SIGINT information will be required to complete the training outlined below which is available on e-Campus or VUport. All training must be completed prior to being granted access to raw SIGINT and annually thereafter:

- (U) OVSC1000, "*NSA/CSS Intelligence Oversight Training*"
- (U) OVSC1100, "*Overview of SIGINT Authorities*"
- (U) OVSC1800, "*Legal Compliance and Minimization Procedures*"

(U//~~FOUO~~) In addition to the above training, all USCYBERCOM, SC, and CNMF personnel supporting cyber operations will be required to complete the following compliance courses related to IAD data:

- (U) OVSC1300, "*Overview of Information Assurance Authorities*" – required annually
- (U) OVSC1400, "*Signals Intelligence and Information Assurance Dual Authorities*"– required every two years

(U//~~FOUO~~) USCYBERCOM and SC CIOOs and auditors will be required to complete the following courses as applicable:

- (U) OVSC2201, "*Intelligence Oversight Officer Training*" – required every two years for those personnel performing CIO duties
- (U) OVSC3101, "*NSA Raw Traffic Database Auditor Training*" – required every two years for those personnel performing auditing duties.

(U//~~FOUO~~) All USCYBERCOM, SC, and CMF personnel, CIOOs and auditors included, working under the SIGINT Operational Control of DIRNSA/CHCSS and accessing Foreign Intelligence Surveillance Act (FISA) Amendment Act (FAA) 702 data will complete OVSC1203, "*Foreign Intelligence Surveillance Act (FISA) Amendment Act (FAA) Section 702*"- required annually.

(U//~~FOUO~~) In addition to the training outlined above, USCYBERCOM, SC, and CMF CIOOs and auditors must complete training to the level of authority approved for that mission.

(U) USCYBERCOM, SC, and CMF personnel assigned as CIOPMs, CIOOs, and auditors will be required to complete CIO familiarization training with experienced NSA/CSS personnel as prescribed by the SID and IAD O&C offices. Additional training will be provided to CIOOs and CIOPMs with unique on-site situations as required. NSA/CSS personnel at NSAW and at the Cryptologic Centers will be available to provide this training as this Implementation Plan begins. Over time, USCYBERCOM, SC, and CMF personnel trained in CIO will be responsible for providing this familiarization training.

(U) On-site CIOOs will work with the CIOPMs to provide remedial training to individuals or groups in response to an IO incident.

(U) All training requirements associated with CIOPM, CIOO, and auditing duties will be established in Job Qualification Requirements (JQR). Personnel assigned such duties will complete all required JQRs before being certified for assignment.

(U) Auditing:

(U//~~FOUO~~) Auditors will acknowledge responsibilities to audit queries via [redacted] or other approved auditing functions. They will conduct daily audits of all assigned personnel and ensure that database queries are valid and compliant with U.S. laws and procedures that govern SIGINT activities. More specifically, auditors must verify that all SIGINT queries have foreign intelligence purposes and do not seek information about U.S. or persons from Australia, Canada, Great Britain, and New Zealand. Auditing responsibilities may vary depending on the data types being queried. As such, auditors must be experienced SIGINT and/or IA analysts, and familiar with the cryptologic mission performed and the NSA/CSS data stores that are used to support the USCYBERCOM and CMF missions. Additionally, auditors should mentor analysts that are assigned to USCYBERCOM and the CMF regarding the proper construction of database queries. Any incidents noted during auditing shall be reported immediately upon recognition to the on-site CIOO, the respective CIOPM, the USCYBERCOM CIOPM, and NSA SV and IV. The incident must be documented in the IO Quarterly report.

(U) Auditors will run monthly workload metrics reports. These reports will assist CIOOs and auditors in ensuring that auditing responsibilities are manageable. CIOOs will meet quarterly with auditors to discuss workloads, determine if the appropriate auditable data stores are being used, and if analysts are succeeding in performing SIGINT activities and Defensive Cyber Operations or encountering challenges. Discussions should inform decisions regarding queries against NSA/CSS data stores, more effective means of querying raw traffic databases, and whether additional auditors are needed.

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

(U) CIO Reporting & CIO Path:

(U) USCYBERCOM must submit two reports in regards to violations and incidents of noncompliance: Incident Reports and CIO Reports.

1. (U) USSID SP0018 incidents and violations involving E.O. 12333 or FISA/FAA material are to be reported to the on-site CIOO immediately upon recognition who will send an e-mail notification regarding the incident to the USCYBERCOM CIOPM [redacted] the SC CIOPM, NSA/CSS IG [redacted] and SV via the Incident Reporting form, and IV (if applicable). The Incident Report template can be found on the SV website. SCs should report incidents in accordance with Service policy.

2. (U) CIO Quarterly Reports will be submitted quarterly to detail recent activities, training statistics, incidents, or CIO related activities. SC CIOOs will provide quarterly reports to their respective CIOPMs, who will review and forward those reports to the USCYBERCOM CIOPM for inclusion in USCYBERCOM CIO Quarterly report. The format for the Quarterly report can be found on the SV website. SCs should provide quarterly reports in accordance with Service policy.

3. (U) Incidents involving the violation of IAD approved procedures shall be recorded and reported within one business day (24 hours – weekend and holidays excluded) of recognition of the event to the USCYBERCOM CIOPM [redacted] the SC CIOPM, NSA/CSS IG [redacted] and IV [redacted]. SCs should report incidents in accordance with Service policy.

4. Incidents involving FAA 702 data will be reported immediately upon recognition to SV [redacted] with a cc to the SID_IG Quarterly alias [redacted] USCYBERCOM CIOPM [redacted] and the SC CIOPM and IV (if applicable). SCs should report such incidents in accordance with Service policy.

(U) Transition Plan:

(U) NSA/CSS Mission Owners that delegate SIGINT mission to USCYBERCOM will mentor, support, and train USCYBERCOM CIOPMs, CIOOs, auditors and support personnel regarding collection, processing, analysis, production, retention, and dissemination of SIGINT, as well as incident reporting and auditing until such time that USCYBERCOM CIO personnel are fully trained and experienced. NSA Mission Owners and O&C organizations at NSAW and the Cryptologic Centers will provide similar support and advice to local SCs (in support of CCMF) and the CNMF. Additionally, NSA/CSS Mission Owners, SV and IV will continue to support USCYBERCOM CIO personnel as needed after CIO responsibility is transitioned to ensure USCYBERCOM compliance with policy and procedures governing SIGINT and IA activities.

(U) Once DIRNSA Mission Delegation is received, USCYBERCOM shall:

- (U) Identify all CIOPMs, CIOOs, and auditors and begin training;
- (U) Have all USCYBERCOM staff, SC and CMF personnel requiring access to SIGINT complete: OVSC1000, OVSC1100, OVSC1300, OVSC1400, OVSC1800, and OVSC1203 for FAA;
- (U) Have all USCYBERCOM, SC, and CMF CIOOs and auditors complete OVSC 2201 (CIOOs), OVSC 3101 (Auditors);(U) Have all USCYBERCOM, SC, and CMF personnel complete necessary courses to perform delegated SIGINT missions (e.g., Smart Targeting Classes: CRSK1300, CRSK1350; RPTG1011, [redacted] (TOOL1200), etc);

(U) NSA, at the Enterprise level, will support USCYBERCOM, SC, and CMF training via:

- SV21and IV Training (OVSC courses, CIO reading, Vuport, Ecampus, [redacted]
- SV21 and IV [redacted] Team (CARS, [redacted] roles/access)
- SV21 Consensual Requests

- SV22 and IV Operations Desk - front door for SID and IAD O&C information respectively
- SV4 NSA FISA, FBI FISA, FAA
- SV31 and IV Incident reporting and CIO Quarterly
- SV32 Super Auditing

(U) Intelligence Oversight Officer Verification Form

(U) This form must be signed and submitted to SID'S Office of Oversight and Compliance (SV) [redacted] prior to mission activation in [redacted] and assuming Intelligence Oversight Officer (IOO) duties.

(U//~~FOUO~~) All IOOs, including those identified on the [redacted] must complete and submit this form when the individual accepts the IOO role. This form, along with a mission's approved mission documentation, replaces the Oversight Implementation Report.

(U//~~FOUO~~[1]) I, _____, the (on-site/off-site[2]) IOO for (organization/element) at (location; [redacted] certify that the intelligence oversight requirements and measures described in USSID SP0019 "*NSA/CSS Signals Intelligence Directorate – Oversight and Compliance Policy*" and IAD MD Number 20, "*IA Oversight and Compliance Program.*" have been implemented and are being adhered to at (location).

__ (U) I am an IOO assigned to a new mission/location

__ (U) I am replacing an IOO on an existing mission/location

_____

CIOO Printed Name, Date

_____

CIOO Signature

[1] (U) Classification should be changed to reflect the sensitivity of the Organization, location and [redacted] if required.

[2] (U) Off-site IOO's must be approved in writing by Chief, Oversight and Compliance and USCYBERCOM CIOPM