January 2, 2019

INS-2018-003

(U) Report of Inspection: The Cyber Threat Intelligence Integration Center (CTIIC), Office of the Director of National Intelligence

~~**Inspector General Sensitive Information**~~

~~(U) This report contains information that the Office of the Inspector General of the Intelligence Community has determined is confidential, sensitive, or protected by Federal Law, including protection from public disclosure under the Freedom of Information Act (FOIA), 5 USC § 552. Recipients may not further disseminate this information without the express permission of the Office of the Inspector General of the Intelligence Community personnel. Accordingly, the use, dissemination, distribution, or reproduction of this information to or by unauthorized or unintended recipients may be unlawful. Persons disclosing this information publicly or to others not having an official need to know are subject to possible administrative, civil, and/or criminal penalties. This report should be safeguarded to prevent improper disclosure at all times. Authorized recipients who receive requests to release this report should refer the requestor to the Office of the Inspector General of the Intelligence Community.~~

Classified By: (b)(3)
Derived From: ODNI CG
Declassify On: 20431231

(U) Mission of the Intelligence Community Inspector General (ICIG)

We conduct independent and objective audits, inspections, investigations, and reviews to promote economy, efficiency, effectiveness, and integration across the Intelligence Community.

(U) To Report Fraud, Waste, and Abuse in Federal Programs

ICIG Hotline
Email: ICIG_HOTLINETEAM (secure); http://www.dni.gov (open)
Telephone: 933-2800 (secure); 1-855-731-3260 (open)

(U) This page intentionally left blank.

(U) Contents

(U) EXECUTIVE SUMMARY

(U) The Cyber Threat Intelligence Integration Center (CTIIC) was established pursuant to a Presidential Memorandum dated February 25, 2015. Among other directives, it required the Director of National Intelligence (DNI) to establish CTIIC for the purpose of producing coordinated Intelligence Community (IC) analysis of foreign cyber threats to U.S. national interests, ensuring that information is shared among the federal cyber community, and supporting the work of operators and policymakers with timely intelligence about significant cyber threats and threat actors.[1]

(U) The July 26, 2016 Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination,* sets forth principles governing the U.S. Government's response to any cyber incident, and directs that: The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the Federal lead agency, during significant cyber incidents, for intelligence support and related activities . . . and is responsible for:

1) Coordinating any multiagency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include relevant Sector Specific Agencies (SSAs) in recognition of their unique expertise;
2) Ensuring that their respective lines of effort are coordinated with other Cyber Unified Coordination Group (UCG) participants and affected entities, as appropriate;
3) Identifying and recommending to the Cyber Response Group (CRG), if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and
4) Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.[2]

(U) The Intelligence Community Inspector General (ICIG) conducted a review of CTIIC. Inspectors evaluated the areas of mission performance, management effectiveness, resource management, and enterprise oversight covering the review period of February 2016 through February 2018.[3]

(U) The results of this review identified seven findings, of which there are five challenges, with nine recommendations, one observation, and one commendable.[4]

[1] (U) Presidential Memorandum, *Establishment of the Cyber Threat Intelligence Integration Center*, February 25, 2015.

[2] (U) Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, July 26, 2016. The PPD sets forth principles governing the Federal Government's response to any cyber incident, and for significant cyber incidents, it establishes lead Federal agencies (ODNI, DOJ, and DHS) and an architecture for coordinating a broader Federal Government response.

[3] (U) ICIG conducted a review in accordance with the Council of Inspectors General on Integrity and Efficiency 2012 *Quality Standards for Inspection and Evaluation*.

[4] (U) ICIG categorizes its findings in the following way: Challenges (identify areas where we recommend action be completed within a specified timeframe upon release of final report, and that will be monitored by the ICIG for completion); Observations (provided for situational awareness); and Commendables (items that highlight efficient and noteworthy ongoing practices).

(U) FINDINGS

Challenge 1	(U) The functions of the National Intelligence Manager for Cyber and CTIIC are not fully consolidated.	Recommendation 1a *(within 90 days)*	[redacted] CTIIC, in coordination with ODNI leadership - Develop and implement a plan to combine all cyber activities, both administratively and functionally, to achieve full integration of cyber intelligence activities, as directed in the FY 2016 IAA.
		Recommendation 1b *(within 90 days)*	(U) ODNI leadership - Review and revise relative ODNI policy and strategic documents to ensure ODNI Mission Center guidance includes CTIIC.
Challenge 2	(U/~~/FOUO)~~ CTIIC and ODNI staffing practices impede the validation of congressionally imposed position limits.	Recommendation 2a *(within 30 days)*	(U) CTIIC, in coordination with ODNI COO - Request that ODNI Office of General Counsel define the term "matrix" and determine its permissibility regarding how those employees are reflected in ODNI official staffing counts.
		Recommendation 2b *(within 45 days)*	(U/~~/FOUO)~~ CTIIC, in coordination with ODNI COO - Provide ICIG an accurate accounting of CTIIC staffing position numbers that align to the congressionally imposed position limits.
Challenge 3	(U) The ratio of Joint Duty Assignment personnel does not align with the ODNI *Strategic Human Capital Plan 2012-2017.*	Recommendation 3 *(within 90 days)*	(U/~~/FOUO)~~ CTIIC, in coordination with ODNI HR - Develop and implement a plan that includes a recruitment strategy to identify potential candidates with the appropriate core competencies to complete the CTIIC mission, and move toward a 50:50 civilian workforce ratio, as targeted in the *Strategic Human Capital Plan 2012-2017*.
Challenge 4	(U) CTIIC is not in full compliance with ODNI Instructions requiring documentation of processes and procedures.	Recommendation 4a *(within 90 days)*	(U) ODNI COO - Conduct an assessment of the ODNI components and centers to determine the inventory of component specific SOPs, evaluate variations and gaps therein, and develop more specific guidance to standardize record keeping requirements.
		Recommendation 4b *(within 90 days)*	(U) CTIIC - Identify, develop, and implement a plan to capture the organization's functions, policies, decisions, and procedures, as required by ODNI Instructions 24.01 and 80.10.
Challenge 5	(U) CTIIC's Threat Opportunity Section (TOS) mission requires clarifying guidance, along with a workforce analysis to determine appropriate spacing needs.	Recommendation 5a *(within 90 days)*	(U/~~/FOUO)~~ CTIIC - Develop and implement a comprehensive plan to maximize the mission effectiveness of TOS, to include the ability to measure product deliverables to the National Security Council Staff or interagency stakeholders. The plan should also include a comprehensive workforce analysis that accounts for the most efficient use of personnel resources.
		Recommendation 5b *(within 60 days)*	(U/~~/FOUO)~~ CTIIC, working with ODNI Facilities Management - Complete the plan to move TOS to the LX facility, based on actual TOS staffing numbers.
Observation	(U) Future Federally Funded Research and Development Center Support to CTIIC may not be required.		
Commendable	(U) The Cyber Threat Intelligence Summary provides valuable information to stakeholders.		

(U) INTRODUCTION

~~(S//NF)~~ The Cyber Threat Intelligence Integration Center (CTIIC) was established pursuant to Presidential Memorandum, *Establishment of the Cyber Threat Intelligence Integration Center*, dated February 25, 2015. Among other responsibilities, CTIIC is tasked with providing integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. National interests. Accordingly, in Fiscal Year (FY) 2015, a CTIIC planning team conducted a workforce analysis and determined it would require (b)(1) full-time equivalent employees to complete CTIIC's mission responsibilities.[5]

(U) Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, sets forth principles governing the Federal Government's response to any cyber incident, whether involving government or private sector entities. PPD-41 further directs that for significant cyber incidents, the Office of the Director of National Intelligence (ODNI), through CTIIC, is to be the lead federal agency for intelligence support and related activities.[6]

(U/~~FOUO~~) CTIIC is located in (b)(3) To execute their mission responsibilities as identified in the listed foundational documents, CTIIC's structure is composed of three sections with distinct responsibilities.

Current Intelligence Section (b)(3) – Build shared situational awareness of significant foreign cyber threats with context, e.g., daily production of the Cyber Threat Intelligence Summary (CTIS);
Analysis Integration Section (b)(3) – Integrate all source IC analysis of foreign cyber adversaries, threats, and incidents; and
Threat Opportunity Section (b)(3) – Support and facilitate interagency development of options by leveraging all instruments of national power.

(U/~~FOUO~~) CTIIC has an association with the National Intelligence Manager for Cyber (NIM-Cyber) with a staff that is administratively connected but functionally separate. The NIM-Cyber is the Director of National Intelligence's Intelligence Community lead for cyber intelligence issues, and is responsible for the integration of IC collection and analysis on cyber issues.

~~(S//NF)~~ Congress expressed concerns in the FY 2016 Intelligence Authorization Act (IAA) regarding the duplication of cyber analysis and missions, and directed the ODNI to consolidate the functions of NIM-Cyber with those of CTIIC.[7]

[5] (U) See Appendix B: CTIIC mission responsibilities as identified in Presidential Memorandum, *Establishment of the Cyber Threat Intelligence Integration Center*, dated February 25, 2015.

[6] (U) The July 26, 2016 Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, states that intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.

[7] (U) FY 2016 IAA – the classified annex to Division M of the Consolidated Appropriations Act of FY 2016 (H.R. 2029).

(U) CTIIC Overview

(U) Scope/Methodology

(U) The Office of the Inspector General of the Intelligence Community conducted a review of CTIIC's management effectiveness, mission performance, resource management, and enterprise oversight for the period of February 2016 through February 2018.

(U) Inspectors conducted this review from March 7, 2018 through May 15, 2018 in accordance with the Council of the Inspectors General on Integrity and Efficiency, 2012 *Quality Standards for Inspection and Evaluation*. Inspectors held 40 interviews, reviewed more than 300 data call submissions, analyzed questionnaire results from employees (government staff and contractors) and federal customers, and conducted independent research.

(U) The results of this review identified seven findings, of which there are five challenges, with nine recommendations, one observation, and one commendable.[8]

[8] (U) ICIG categorizes its findings in the following way: Challenges (identify areas where we recommend action be completed within a specified timeframe upon release of final report, and be monitored by the ICIG for completion); Observations (provided for situational awareness); and Commendables (items that highlight efficient and noteworthy ongoing practices).

Results of Review

Challenge 1:
(U/~~/FOUO)~~ The Functions of the National Intelligence Manager for Cyber and CTIIC are not fully consolidated

(U) The ODNI includes four mission centers: the National Counterterrorism Center (NCTC), the National Counterintelligence and Security Center (NCSC), the National Counterproliferation Center (NCPC), and CTIIC.

(U) In 2011, the DNI issued a memorandum, 2011-ES-00076, delegating authority to oversee and integrate all aspects of IC collection and analytic efforts against a particular region or function. This memorandum further delegated relative NIM authority to the directors of NCTC, NCSC, and NCPC to ensure the ODNI would be optimally structured to perform these IC functions in the most effective and efficient manner. CTIIC was not included in this memorandum because it was not formally established as a Mission Center until 2015.[9, 10]

~~(S//NF)~~ Moreover, through the FY 2016 IAA, Congress expressed concerns regarding the duplication of cyber analysis and missions, and directed ODNI to consolidate the functions of the NIM-Cyber with CTIIC. This consolidation is comparable to the relationship of the other ODNI Mission Centers to their respective NIMs, as outlined in the DNI memorandum. As of the time of this review, the functions of the NIM-Cyber and CTIIC were not fully consolidated.[11]

Recommendation 1a:
(U) Within 90 days

~~(S//NF)~~ CTIIC, in coordination with ODNI leadership - Develop and implement a plan to combine all cyber activities, both administratively and functionally, to achieve full integration of cyber intelligence activities, as directed in the FY 2016 IAA.

Recommendation 1b:
(U) Within 90 days

(U/~~/FOUO)~~ ODNI COO, in coordination with CTIIC - Review and revise relative ODNI policy and strategic documents to ensure ODNI Mission Center guidance includes CTIIC.

[9] (U/~~/FOUO)~~ ODNI's Integrated Mission Strategy (November 15, 2016) defines a National Intelligence Manager (NIM) as the focal point for IC-wide integration and crisis management across geographic regions worldwide, functional areas, and domains. NIMs promote long-term integration of collection, analysis, and counterintelligence programs, and they provide mission-focused inputs to intelligence planning, budgeting, and priorities.

[10] (U) DNI Memorandum, *Delegation of Certain Authorities and Responsibilities of the DNI for Leadership of the Intelligence Community*, August 28, 2011, E/S 00076. Furthermore, on July 10, 2017, the ODNI CMO, through email, re-designated the terms "National Counterintelligence Executive" (NCIX) and the "Office of the National Counterintelligence Executive" to be formally replaced with the "Director of the National Counterintelligence and Security Center" and the "National Counterintelligence and Security Center," respectively.

[11] (U) The ODNI implemented its transformation plan on July 25, 2018, and included both an organizational and functional realignment across the ODNI. Due to time and scope limitations, the ICIG did not reassess potential impact and changes resulting from this transformation.

Challenge 2:
(U) CTIIC and ODNI staffing practices impede the validation of congressionally imposed position limits

~~(S//NF)~~The FY 2016 IAA directed the ODNI to consolidate the functions of the NIM-Cyber with those of CTIIC, and further stipulated that any of the positions moved from the NIM-Cyber would not be counted against CTIIC's (b)(1) position limit.[12]

(U) Inspectors reviewed staffing documents provided by both ODNI Human Resources (HR) and CTIIC (inclusive of NIM-Cyber), and analyzed Memorandums of Understanding (MOUs) and staffing rosters in an attempt to confirm CTIIC's staffing position count. However, the staffing rosters varied and could not be reconciled.

(U/~~FOUO~~) ICIG inspectors further identified MOUs for (b)(3) Joint Duty Assignment (JDA) employees from the Federal Bureau of Investigation. Those JDAs were working at CTIIC, yet their staffing positions were reflected as working for NCTC. Another (b)(3) MOUs for personnel working at CTIIC were categorized as "matrixed," yet none of those positions were counted against CTIIC's staffing position limit.[13]

(U) Due to the listed discrepancies, and use of the ambiguous term "matrixed" employees, inspectors were unable to verify CTIIC's actual staffing number and compliance with congressionally imposed staffing limits. Analysis of the data collected, as of February 25, 2018, is shown in Table 1, and further reflects the inconsistencies in staff position numbers for CTIIC.[14]

~~(S//NF)~~Table 1.

	ODNI Staffing Table	CTIIC Staffing Chart
ODNI Cadre	(b)(1)	[redacted]
Joint Duty Assignment	[redacted]	[redacted]
Assignees	[redacted]	[redacted]
US Military	[redacted]	[redacted]
Contractors	[redacted]	[redacted]
Vacancies	[redacted]	[redacted]
Matrix	[redacted]	[redacted]
CTIIC Total *excluding NIM-Cyber*	[redacted]	[redacted]
CTIIC Total *including NIM-Cyber*	[redacted]	[redacted]

Recommendation 2a:
(U) Within 30 days

(U) CTIIC, in coordination with ODNI COO – Request that ODNI Office of General Counsel define the term "matrix" and determine its permissibility regarding how those employees are reflected in ODNI official staffing counts.

Recommendation 2b:
(U) Within 45 days

(U) CTIIC, in coordination with ODNI COO – Provide ICIG an accurate accounting of CTIIC staffing position numbers that align to the congressionally imposed position limits.

[12] ~~(S//NF)~~The FY 2016 IAA reflects a position count of (b)(1) for NIM-Cyber.

[13] (U) ICIG inspectors were not able to locate an official definition of the term "matrix"; therefore, for the purposes of this report, "matrix" is a term used within the ODNI that appears on MOUs to identify staff that are functionally assigned to one ODNI component, but administratively charged to another.

[14] (U) ODNI's use of "matrixed" employees is not limited to CTIIC. During the course of the review, inspectors discovered that other ODNI components are also utilizing "matrixed" employees.

Challenge 3:
(U) The ratio of Joint Duty Assignment personnel does not align with the ODNI Strategic Human Capital Plan 2012-2017

(U/~~FOUO~~) The ODNI *Strategic Human Capital Plan 2012-2017* identified a goal of a 50:50 ratio of cadre to JDA personnel. As of March 2018, the ratio of cadre to JDA for CTIIC was 29:71. The other three ODNI Mission Centers averaged a cadre to JDA ratio of 44:54. As of March 23, 2018, Table 2 summarizes the four ODNI Mission Centers' cadre to JDA ratios.[15]

(U/~~FOUO~~) Table 2.

Mission Center	Cadre	JDA
NCTC	38%	60%
NCSC	47%	52%
NCPC	48%	50%
CTIIC	**29%**	**71%**

(U/~~FOUO~~) An HR document revealed nearly half of CTIIC's detailees are scheduled to depart between FY18-Q4 and FY19-Q2. Interviewees voiced concerns that the lack of continuity of ODNI cadre, and frequent turnover and rotation of detailees, could disrupt the execution of CTIIC mission responsibilities.

Recommendation 3:
(U) Within 90 days

(U/~~FOUO~~) CTIIC, in coordination with ODNI HR – Develop and implement a plan that includes a recruitment strategy to identify potential candidates with the appropriate core competencies to complete the CTIIC mission, and move toward a 50:50 civilian workforce ratio, as targeted in the *Strategic Human Capital Plan 2012-2017*.

[15] (U) ODNI *Strategic Human Capital Plan 2012-2017* states the ODNI will increase workforce competencies in the core occupations consistent with mission-based position requirements and merit principles for selection.

Challenge 4:
(U) CTIIC is not in full compliance with ODNI Instructions requiring documentation of processes and procedures

(U) ODNI Instruction 24.01, *ODNI Internal Control Program*, requires the establishment of "mechanisms to document the risks associated with key areas of the programs, operations, and financial and support activities within their areas of responsibility, and delineate internal control techniques to be used to address those risks." ODNI Instruction 80.10 provides requirements for "ensuring that adequate and proper documentation is created and maintained in established recordkeeping systems to document policies, decisions, procedures, and essential transactions."

(U/~~FOUO~~) CTIIC notes in its strategy document, Plan to Advance CTIIC 2, the need to develop written procedures and directs the action to document applicable business processes, and assigns responsibility for written processes to sub-components within the organization. In response to the ICIG data call, CTIIC provided the ICIG with five Standard Operating Procedures (SOPs) for review that codified only a few of CTIIC's procedures. For example, one SOP explained a procedure for the in-processing of new staff, but not one for out-processing. Moreover, as noted above, CTIIC has a 71:29 JDA to cadre ratio, which necessitates the importance of having a fully documented procedure to assist rotational personnel who may not be aware of processes that govern day-to-day operations of an unfamiliar organization.

(U/~~FOUO~~) On a related note, during previous inspections of ODNI components, ICIG inspectors found that documented procedures below the ODNI Instruction level varied significantly between offices. As the ODNI implements the Transformation, it may benefit the organization to standardize policy and procedures at the Directorate and Center level to facilitate administrative regularity.

(U) The ICIG is aware that CTIIC was stood-up in an expedited fashion to meet statutory requirements. Now in its third year, CTIIC would improve the efficiency of its operations by documenting organizational procedures to fill voids where additional or amplifying guidance is necessary.

Recommendation 4a:
(U) Within 90 days

(U) ODNI COO – Conduct an assessment of the ODNI components and centers to determine the inventory of component specific SOPs, evaluate variations and gaps therein, and develop more specific guidance to standardize record keeping requirements.

Recommendation 4b:
(U) Within 90 days

(U) CTIIC – Identify, develop, and implement a plan to capture the organization's functions, policies, decisions, and procedures, as required by ODNI Instruction 80.10.

[16] (U) ODNI Instruction 24.01, *ODNI Internal Control Program*, Dec 18, 2012 and ODNI Instruction 80.10, *Creation of the Office of the Director of National Intelligence Records*, Aug 31, 2010.

Challenge 5:

(U) CTIIC's Threat Opportunity Section mission requires clarifying guidance, along with a workforce analysis to determine appropriate spacing needs

(U/~~FOUO~~) CTIIC mission responsibilities are identified in both Presidential Memorandum dated February 25, 2015, *Establishment of the Cyber Threat Intelligence Integration Center* and PPD-41. In order to execute these mission responsibilities, CTIIC leadership established three sections with different responsibilities: Current Intelligence Section (CIS), Analysis Integration Section (AIS), and Threat Opportunity Section (TOS). Inspectors found the functions of CIS and AIS are more specific, whereas the TOS mission is not. TOS is charged with facilitating and supporting USG responses to cyber threats by working with policy and operational stakeholders to identify and integrate the range of response options, along with accompanying considerations policymakers require to decide on courses of action. To accomplish these tasks, TOS officials said they have a (b)(3) person team that develops products such as strategic assessments of USG cyber plans and policies, USG cyber response options matrices, USG courses of actions, and occasional memorandums and working papers, to support the needs of the National Security Council Staff (NSCS).

(U/~~FOUO~~) ICIG inspectors interviewed NSCS to determine whether TOS is effective in the implementation of its cyber facilitation and support functions, as prescribed by internal mission guidance documents. While ICIG inspectors found there is a relationship between TOS and the NSCS, evidence revealed a low demand and limited interest for TOS products by NSCS.

(U) The following chart depicts information received throughout the course of our review regarding TOS developed products and their usability.

(U/~~FOUO~~) Table 3.

Products developed by TOS	Customer	Frequency	Personnel required
Strategic Assessments	NSCS	None completed	1 person per assessment
Option Matrices	NSCS	Approx. 6 over the past 2.5 years	1 person per matrix
Courses of Action (COA)	NSCS	Approx. 4 over the past 2.5 years	1 person per COA
Work Papers	NSCS	Occasionally as needed	1 person per work paper

(U/~~FOUO~~) General comments revealed a range of opinions regarding TOS mission performance. One senior official said TOS could do a better job integrating with NSCS personnel to better understand customer needs. It was further indicated that TOS is having a difficult time carving out mission space as a result of more established USG cyber centers producing similar products. The general sentiment was that TOS products are duplicative and of limited informational value.

(U/~~/FOUO)~~ Another official said there are broader factors that contribute to the uncertainty of the TOS mission, such as unclear mission guidance from internal leadership and conflicting direction within the organization. Yet another attributed the mission uncertainty to a breakdown in communication as a result of TOS not being co-located with the rest of CTIIC.

(U/~~/FOUO)~~ TOS is physically located in the Intelligence Community Campus-Bethesda, in a secure work space built and furnished to accommodate (b) (3) work stations, apart from the rest of CTIIC; however, TOS only has (b) (3) occupied workstations, leaving a 60 percent surplus of work space.

(U/~~/FOUO)~~ It should be noted that CTIIC has plans to consolidate all mission activities and move TOS personnel to the (b)(3) as part of the ongoing ODNI transformation activities. Although we are encouraged to hear that planning efforts are underway to achieve greater efficiencies through a consolidation of personnel, such plans have not been completed to date.

Recommendation 5a:
(U) Within 90 days

(U/~~/FOUO)~~ CTIIC – Develop and implement a comprehensive plan to maximize the mission effectiveness of TOS, to include the ability to measure product deliverables to the National Security Council Staff or interagency stakeholders. The plan should also include a comprehensive workforce analysis that accounts for the most efficient use of personnel resources.

Recommendation 5b:
(U) Within 60 days

(U/~~/FOUO)~~ CTIIC, working with ODNI Facilities Management – Complete the plan to move TOS to the (b)(3), based on actual TOS staffing numbers.

Observation:
(U) Future Federally Funded Research and Development Center support to CTIIC may not be required

(U/~~FOUO~~) Through a Federally Funded Research and Development Center (FFRDC), CTIIC is developing an analytic prototype tool that should be released for commercial contractor bidding upon completion. CTIIC leadership justification for using an FFRDC is to mitigate concerns that a commercial contractor may gain a competitive advantage if follow-on work is awarded.

(U) In the event follow-on support is needed, CTIIC should consider a detailed assessment, consistent with Federal Acquisition Regulations § 35.017, that includes assessing whether mission needs necessitate the use of an FFRDC.[17]

Commendable:
(U/~~FOUO~~) The Cyber Threat Intelligence Summary provides valuable information to stakeholders

(U) CTIIC produces seven products, including but not limited to the Cyber Threat Intelligence Summary (CTIS), which CTIIC considers a cornerstone of its mission. The CTIS provides threat reporting plus context, commentary, and IC/USG actions. It also highlights intelligence and finished community analysis from around the IC. CTIS customers include Federal Cyber Centers, the IC, and National Security Council Staff.

(U/~~FOUO~~) The Inspections team disseminated a questionnaire to 935 customer email addresses provided by CTIIC to assess the value of the CTIS.[18]

- *"I find the CTIIC CTIS a great source for cyber threat reporting…";*
- *"This product is invaluable to remain aware of cyber developments globally. There is no other holistic insight product that even comes close to CTIIC…CTIIC is the standard that others seek to achieve";*
- *"The CTIS is an excellent, easily digestible product in providing information on cyber incidents and intelligence reporting related to cyber"; and*
- *"The CTIS is one of the first things I read each morning and it prevents me from having to reach out to multiple agencies for information."*

(U) The ICIG commends CTIIC for its Cyber Threat Intelligence Summary product.

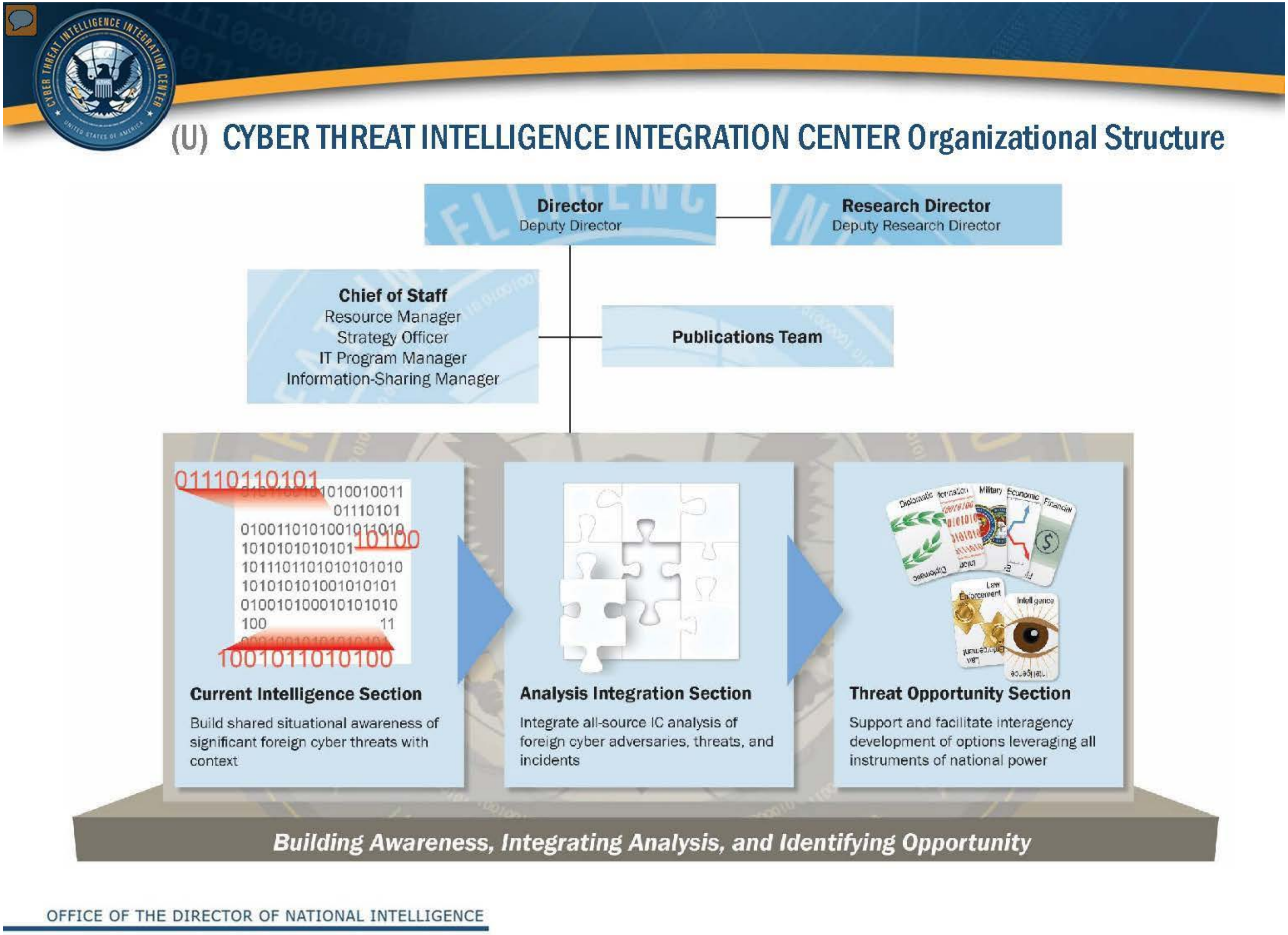
[17] (U) 48 CFR 35.017 sets forth Federal policy regarding the establishment, use, review, and termination of FFRDCs and related sponsoring agreements.

[18] (U/~~FOUO~~) Some email addresses were duplicates or were also included in group email addresses so fewer than 935 individual customers received the questionnaire.

APPENDICES

(U) Appendix A: CTIIC Organizational Chart (as of March 7, 2018)

(U)



(U) CYBER THREAT INTELLIGENCE INTEGRATION CENTER Organizational Structure

Director
Deputy Director

Research Director
Deputy Research Director

Chief of Staff
Resource Manager
Strategy Officer
IT Program Manager
Information-Sharing Manager

Publications Team

Current Intelligence Section
Build shared situational awareness of significant foreign cyber threats with context

Analysis Integration Section
Integrate all-source IC analysis of foreign cyber adversaries, threats, and incidents

Threat Opportunity Section
Support and facilitate interagency development of options leveraging all instruments of national power

Building Awareness, Integrating Analysis, and Identifying Opportunity

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

(U) Appendix B: CTIIC mission responsibilities as identified in Presidential Memorandum, *Establishment of the Cyber Threat Intelligence Integration Center*, dated February 25, 2015.

1. (U) Provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests;

2. (U) Support the National Cybersecurity and Communications Integration Center, the National Cyber Investigative Joint Task Force, U.S. Cyber Command, and other relevant United States Government entities by providing access to intelligence necessary to carry out their respective missions;

3. (U) Oversee the development and implementation of intelligence sharing capabilities (including systems, programs, policies, and standards) to enhance shared situational awareness of intelligence related to foreign cyber threats and incidents affecting U.S. national interests;

4. (U) Ensure that indicators of malicious cyber activity and, as appropriate, related threat reporting contained in intelligence channels are downgraded to the lowest classification possible for distribution to both United States Government and U.S. private sector entities through the mechanism described in section 4 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity); and

5. (U) Facilitate and support interagency efforts to develop and implement coordinated plans to counter foreign cyber threats to U.S. national interests using all instruments of national power, including diplomatic, economic, military, intelligence, homeland security, and law enforcement activities.

(U) Appendix C: The July 26, 2016, Presidential Policy Directive 41*, United States Cyber Incident Coordination*, Section V. Architecture of Federal Government Response Coordination for Significant Cyber Incidents.[19]

(U) The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the Federal lead agency for intelligence support and related activities:[20]

1. Coordinating any multiagency threat or asset response activities to provide unity of effort, to include coordinating with any agency providing support to the incident, to include relevant sector-specific agencies in recognition of their unique expertise;

2. Ensuring that their respective lines of effort are coordinated with other Cyber Unified Coordination Group (UCG) participants and affected entities, as appropriate;

3. Identifying and recommending to the Cyber Response Group, if elevation is required, any additional Federal Government resources or actions necessary to appropriately respond to and recover from the incident; and

4. Coordinating with affected entities on various aspects of threat, asset, and affected entity response activities through a Cyber UCG, as appropriate.

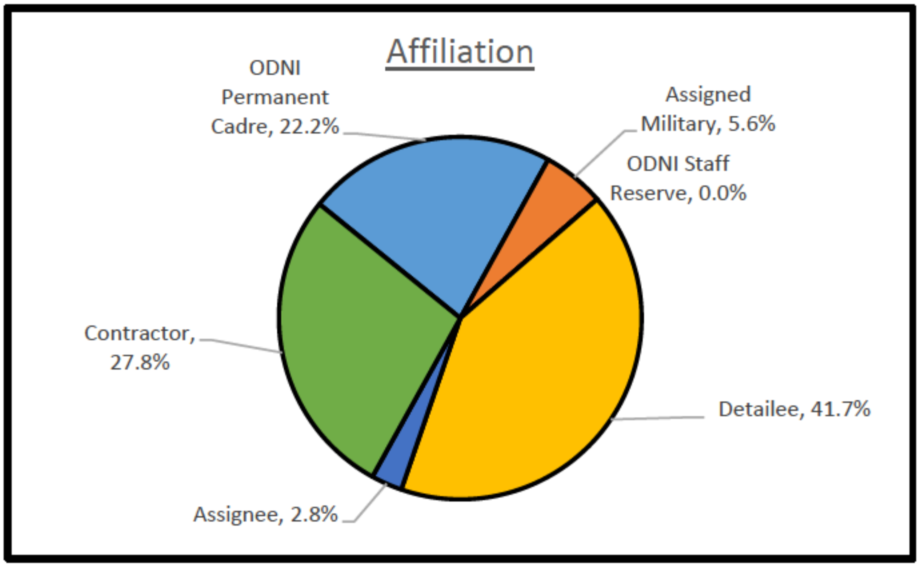
[19] (U) Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, July 26, 2016, establishes Federal lead agencies to ensure maximum effectiveness in coordinating responses to significant cyber incidents: The Department of Justice, acting through the Federal Bureau of Investigation; the Department of Homeland Security, acting through the National Cybersecurity and Communications Integration Center; and the Office of the Director of National Intelligence, acting through the Cyber Threat Intelligence Integration Center.

[20] (U) Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, July 26, 2016, IV. Concurrent Lines of Effort, C. "Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities."

(U) Appendix D: Component Questionnaire Results

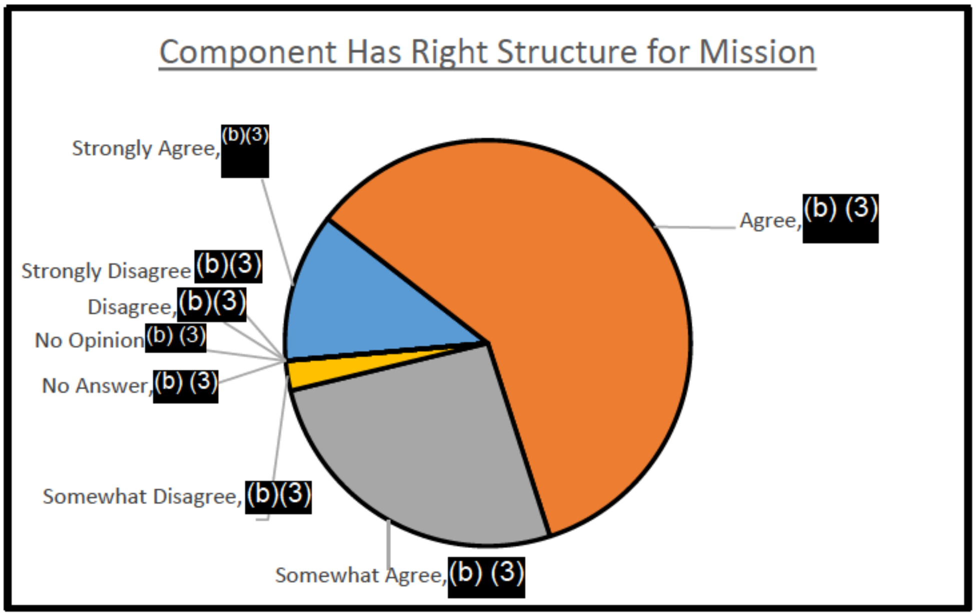
(U) The Inspections team provided CTIIC personnel with a questionnaire that included both open-ended and interval scale prompts. These prompts spanned mission, management, resources, and morale. The following charts represent a sampling of the prompts and responses from the component questionnaire.

(U) Figure 1. Organizational Affiliation

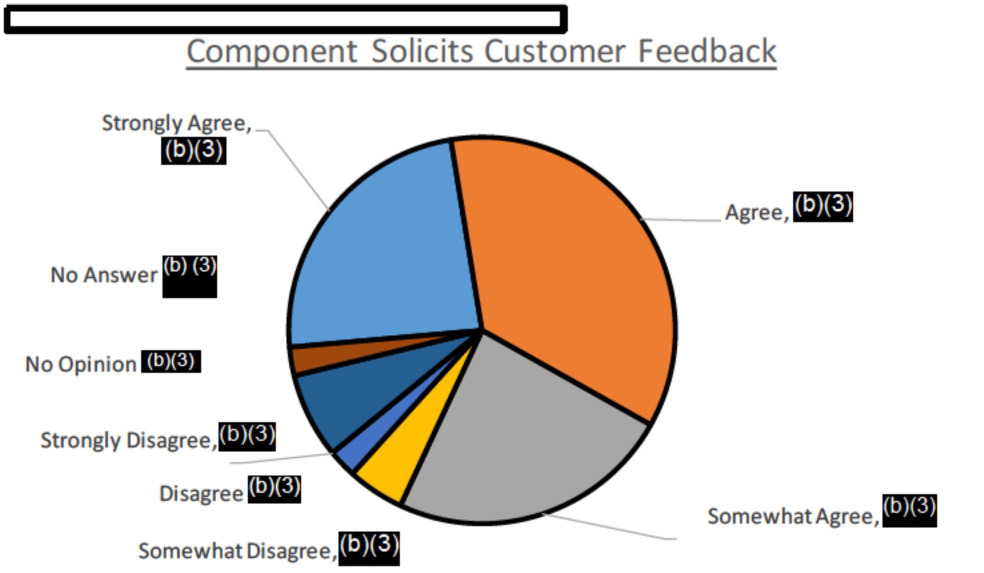


(U//~~FOUO~~) (b) (3) personnel (~75%) responded to the majority of the survey, (b) (3) (~64%) completed it. (b) (3) respondents identified an organizational affiliation, of which 72.2% were government (cadre, detailee, assignee, or military) and 27.8% were contractors.

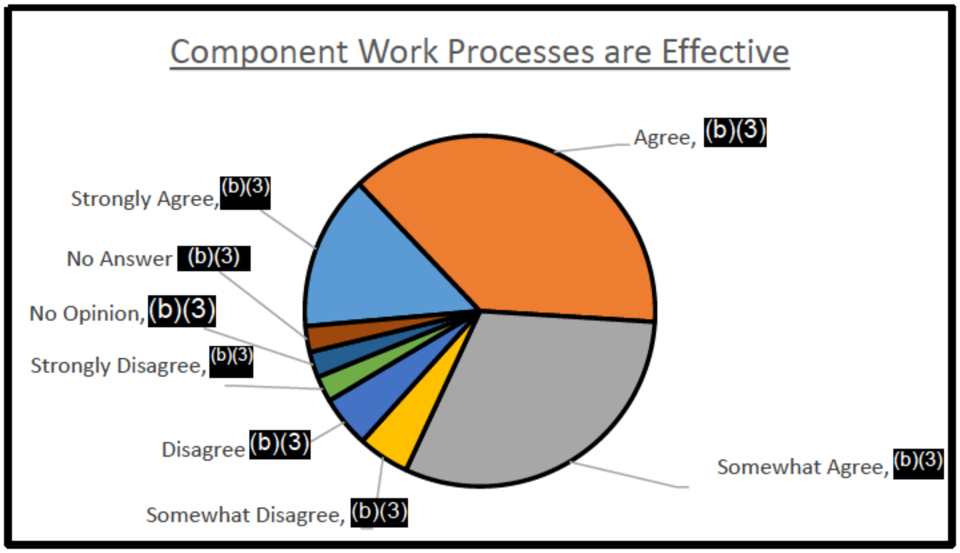
(U) Figure 2. The organizational structure in my component is well suited for performing the mission of the component.



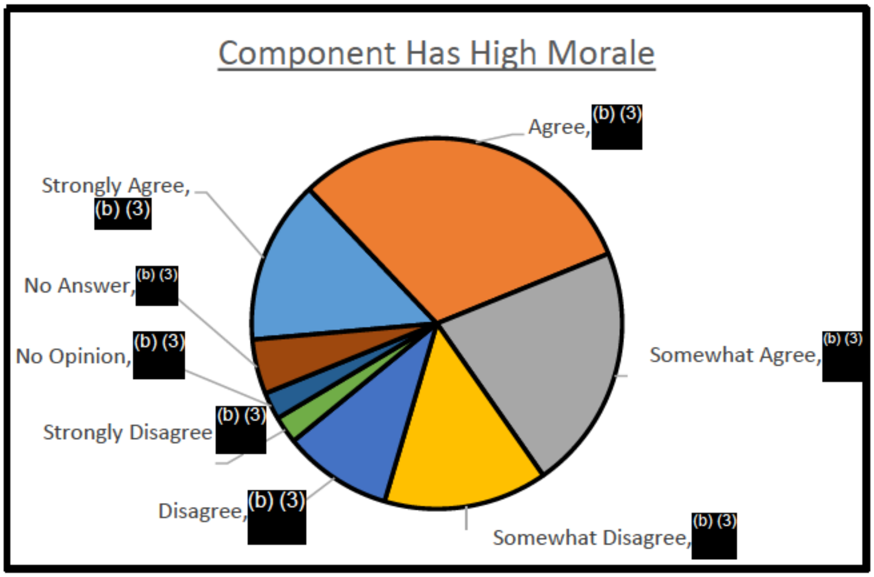
(U) Figure 3. My component solicits formal feedback from customers on the products and services we provide to them.



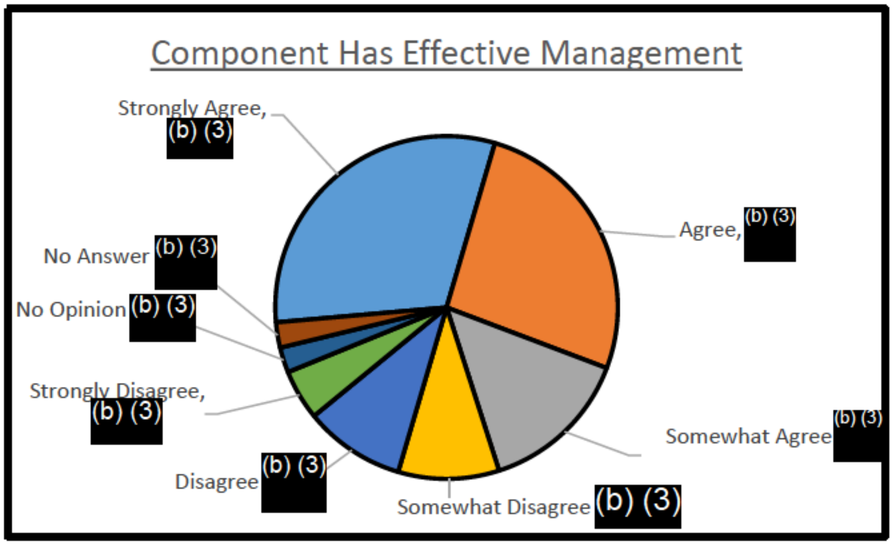
(U) Figure 4. My component's work processes are effective.



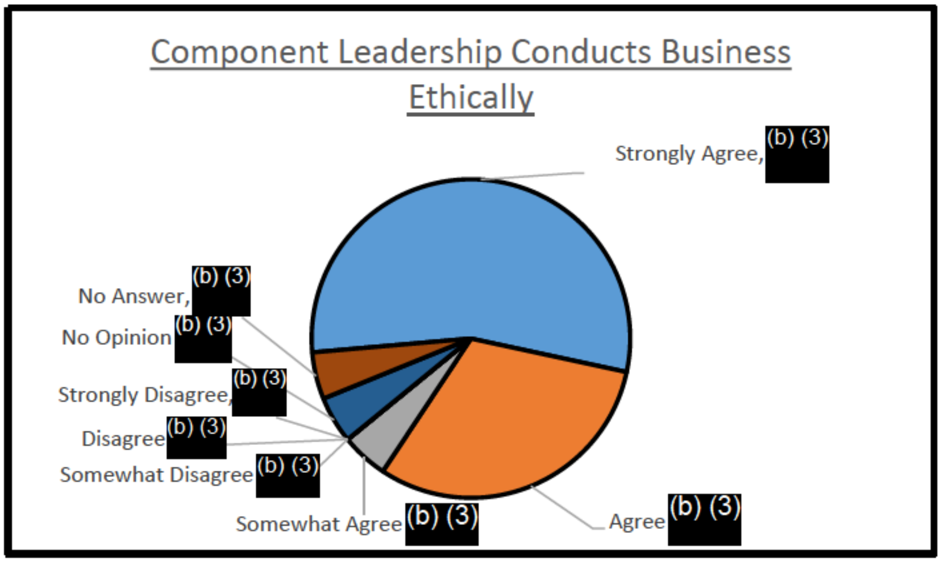
(U) **Figure 5.** My component has high morale.



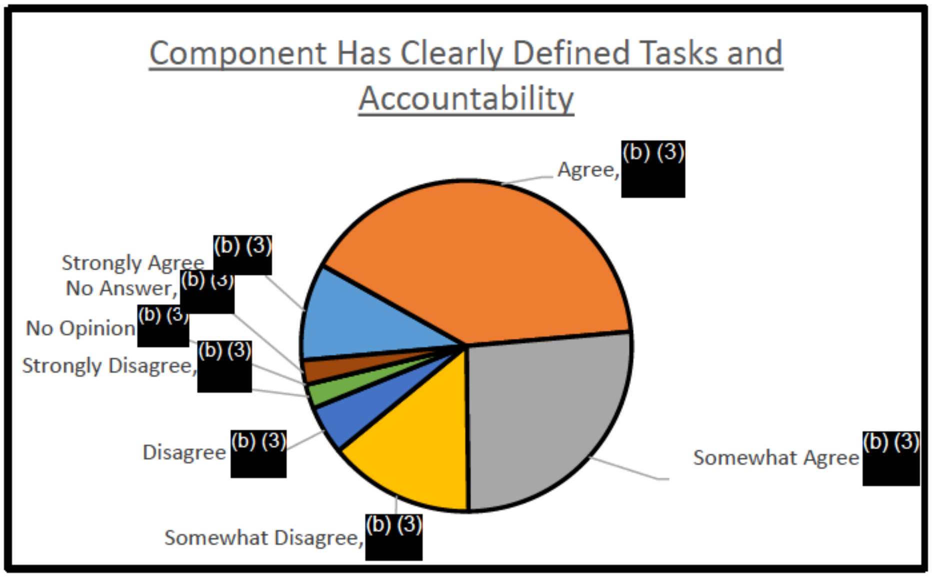
(U) **Figure 6.** My component has effective management at the component level.



(U) Figure 7. Leadership in my component conducts business in an ethical manner.

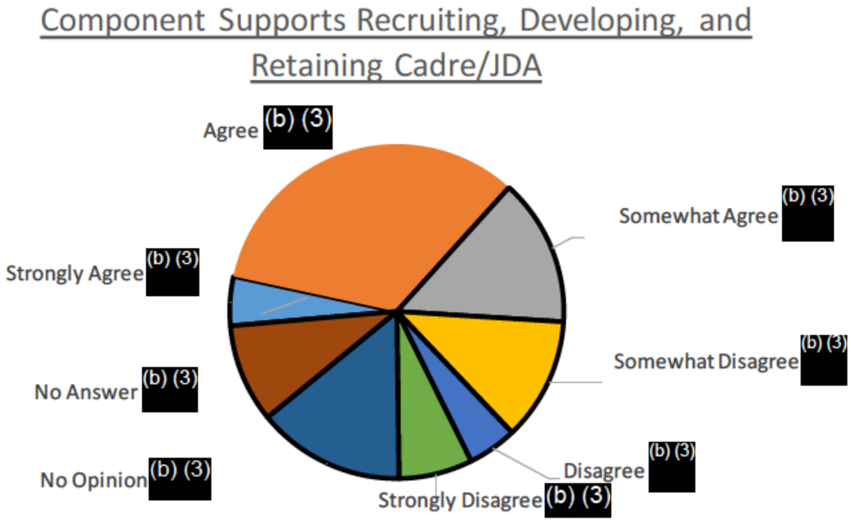


(U) Figure 8. My component has clearly defined tasks and accountability.



(U) Figure 9. ODNI and component personnel practices (including hiring) support the recruitment, development, and retention of cadre and detailees.

[redacted]

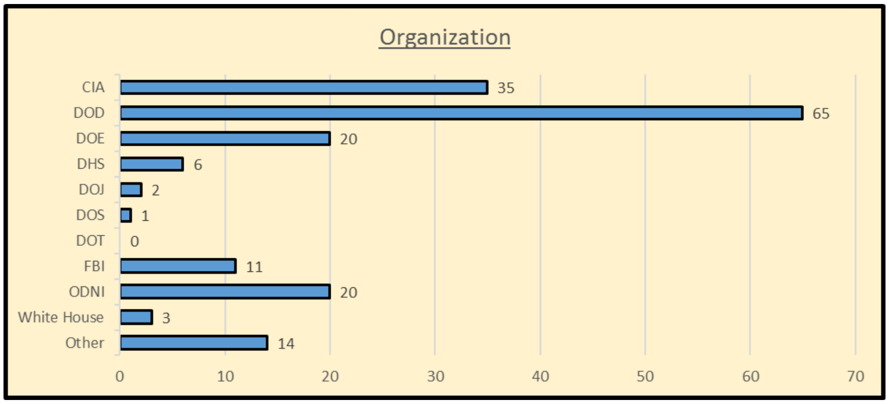


(U) Appendix E: CTIIC Customer Questionnaire Results

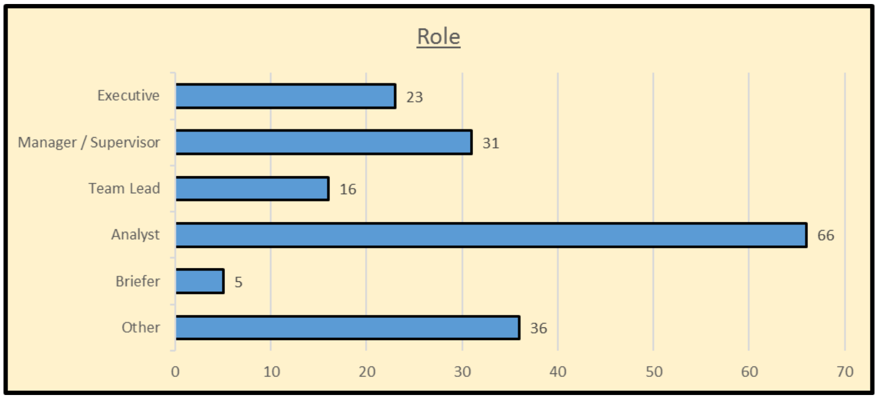
(U) The Inspections team disseminated a questionnaire to 935 customer email addresses provided by CTIIC to assess the value of their flagship project, the CTIS, and received 177 responses. These questions spanned product usage, value, and timeliness, as well as CTIIC staff responsiveness to inquiries.

(U) Of the 177 respondents to the questionnaire, 78.5% were government (cadre, detailee, assignee, or military) and 21.5% were contractors. DoD, as the largest customer element responding to our questionnaire, indicated the most use of the CTIS.

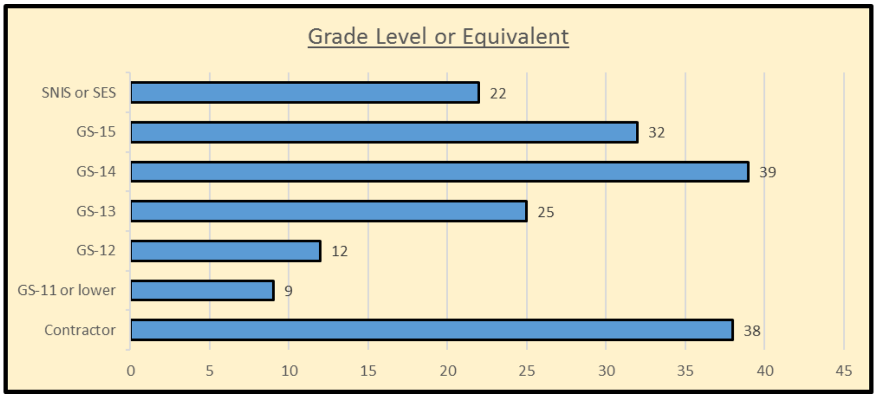
(U) Figure 1. Organizational Affiliation



(U) Figure 2. What role do I hold at my home organization?



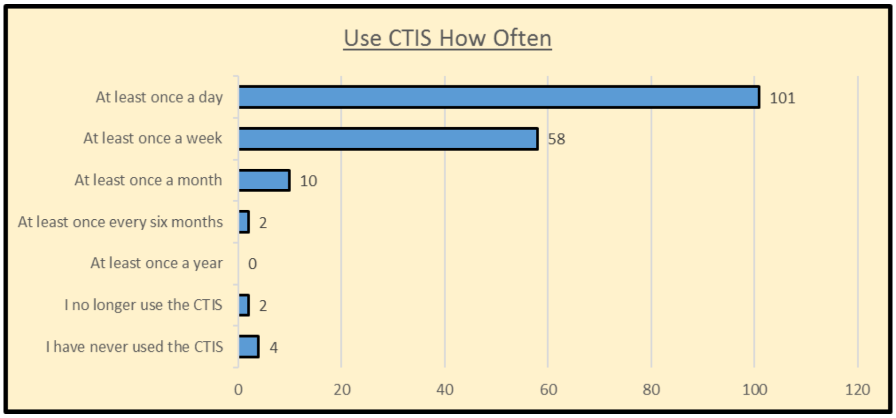
(U) Figure 3. What is your grade level or equivalent?



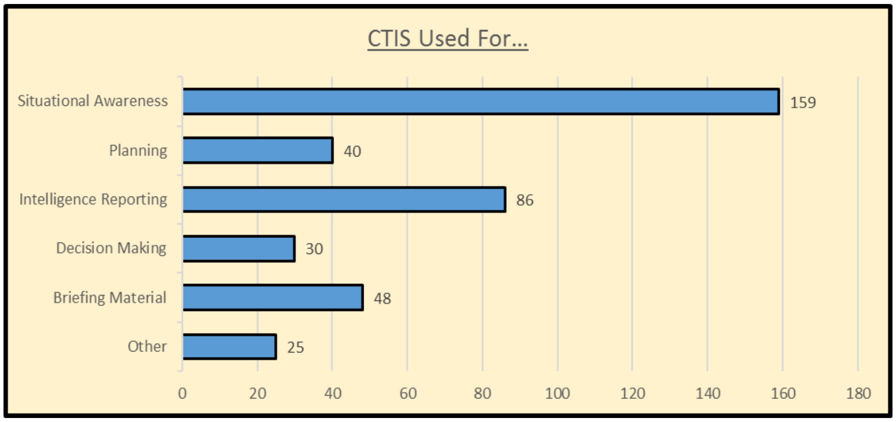
(U) As shown in Figures 2 and 3 above, CTIIC has a broad outreach to varying levels of customers ranging from analyst to executive leadership, and at all levels across the government, including contractor staff.

(U) Figure 4 demonstrates CTIIC products are used daily by more than 1/2 of the respondents. Additionally, more than 2/3 of the respondents use the CTIS at least once a week.

(U) Figure 4. I use the CTIIC CTIS this often:

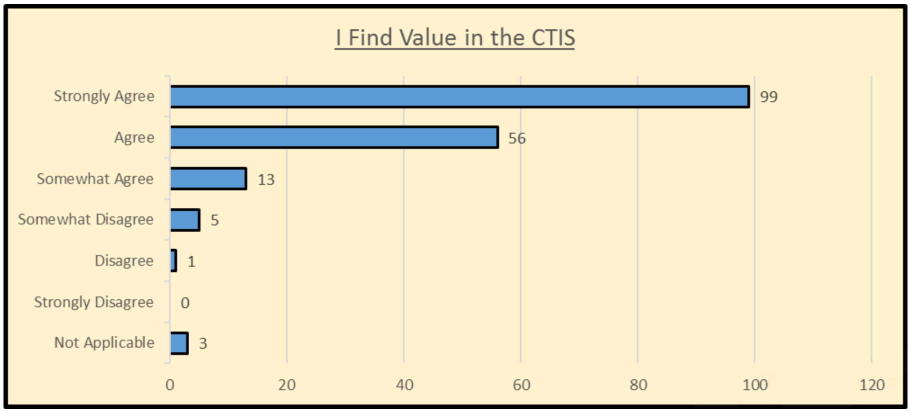


(**U) Figure 5.** I use the CTIS for:



(U) Figure 5 shows the multiple uses and applications of the CTIS among the respondents.

(U//~~FOUO)~~Figure 6. I find value in the CTIIC CTIS product.

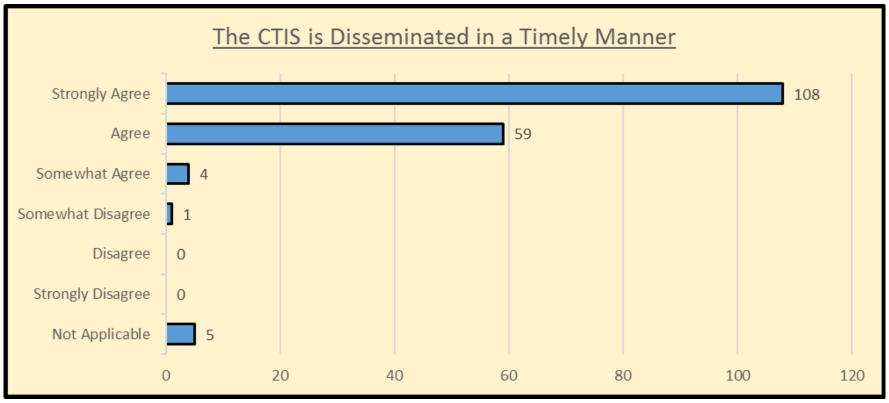


(U) Figure 6 demonstrates the vast majority of respondents find the CTIS a valuable cyber intelligence product that includes both warnings and assessments conducted by experts throughout the IC cyber community.

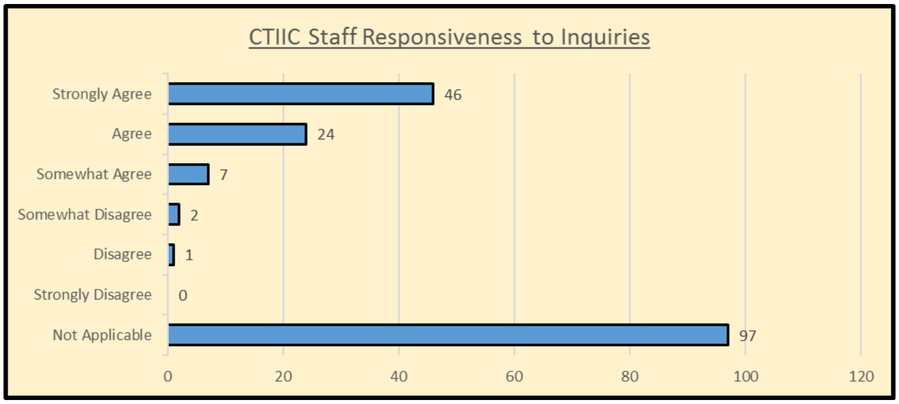
(U) As evident in Figure 7, the majority of respondents feel they receive the CTIS in a timely manner. The CTIS is a summary product typically disseminated two to three times a week.

(U) Figure 8 demonstrates the majority of the respondents did not reach back to CTIIC. However, for customers who indicated having additional inquiries related to CTIIC products, 77 of the 80 noted they receive an acceptable level of response.

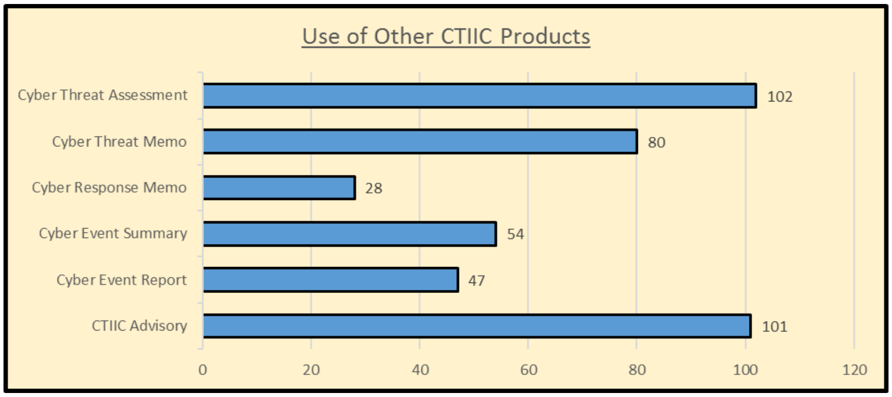
(U) Figure 7. The CTIIC CTIS is disseminated in a timely manner.



(U) Figure 8. The CTIIC staff is responsive to my inquiries.



(U) Figure 9. I have made use of the other CTIIC product:

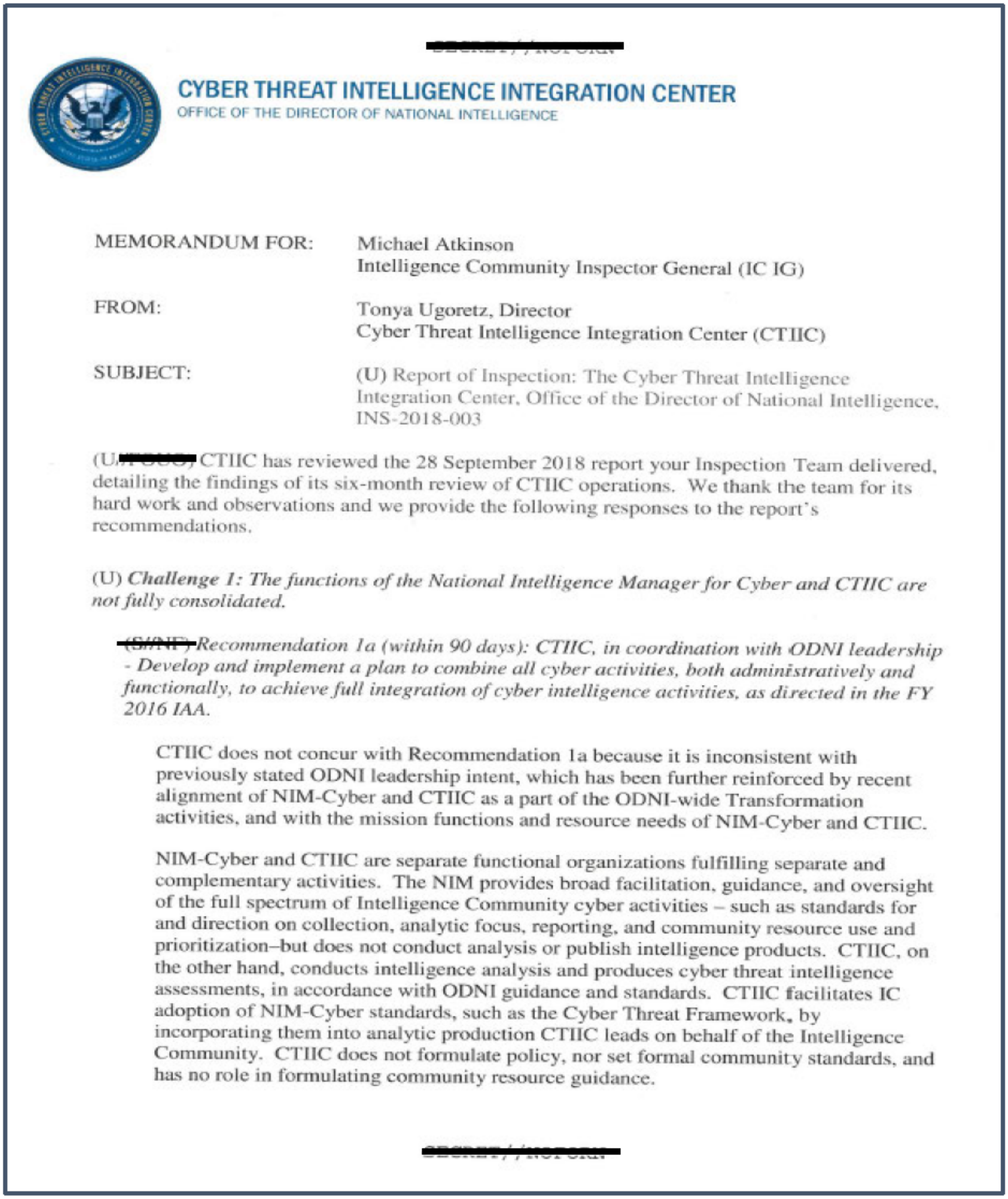


(U) As shown in Figure 9, respondents' use is not limited to the CTIS.

(U) Appendix F: Acronym List

AIS	Analysis Integration Section
CIS	Current Intelligence Section
COA	Course of Action
COO	Chief Operating Officer
CRG	Cyber Response Group
CTIIC	Cyber Threat Intelligence Integration Center
CTIS	Cyber Threat Intelligence Summary
DNI	Director of National Intelligence
FFRDC	Federally Funded Research and Development Center
FY	Fiscal Year
HR	Human Resources
IAA	Intelligence Authorization Act
IC	Intelligence Community
ICC-B	IC Campus-Bethesda
ICIG	Intelligence Community Inspector General
JDA	Joint Duty Assignment
LX	Liberty Crossing
MOU	Memorandum of Understanding
NCPC	National Counterproliferation Center
NCSC	National Counterintelligence and Security Center
NCTC	National Counterterrorism Center
NIM	National Intelligence Manager
NIM-Cyber	National Intelligence Manager for Cyber
NSCS	National Security Council Staff
ODNI	Office of the Director of National Intelligence
PPD	Presidential Policy Directive
SOP	Standard Operating Procedure
SSA	Sector Specific Agencies
TOS	Threat Opportunity Section
USG	United States Government

(U) Appendix G: CTIIC Response



[redacted]

CYBER THREAT INTELLIGENCE INTEGRATION CENTER
OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

MEMORANDUM FOR: Michael Atkinson
Intelligence Community Inspector General (IC IG)

FROM: Tonya Ugoretz, Director
Cyber Threat Intelligence Integration Center (CTIIC)

SUBJECT: (U) Report of Inspection: The Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence, INS-2018-003

(U[redacted] CTIIC has reviewed the 28 September 2018 report your Inspection Team delivered, detailing the findings of its six-month review of CTIIC operations. We thank the team for its hard work and observations and we provide the following responses to the report's recommendations.

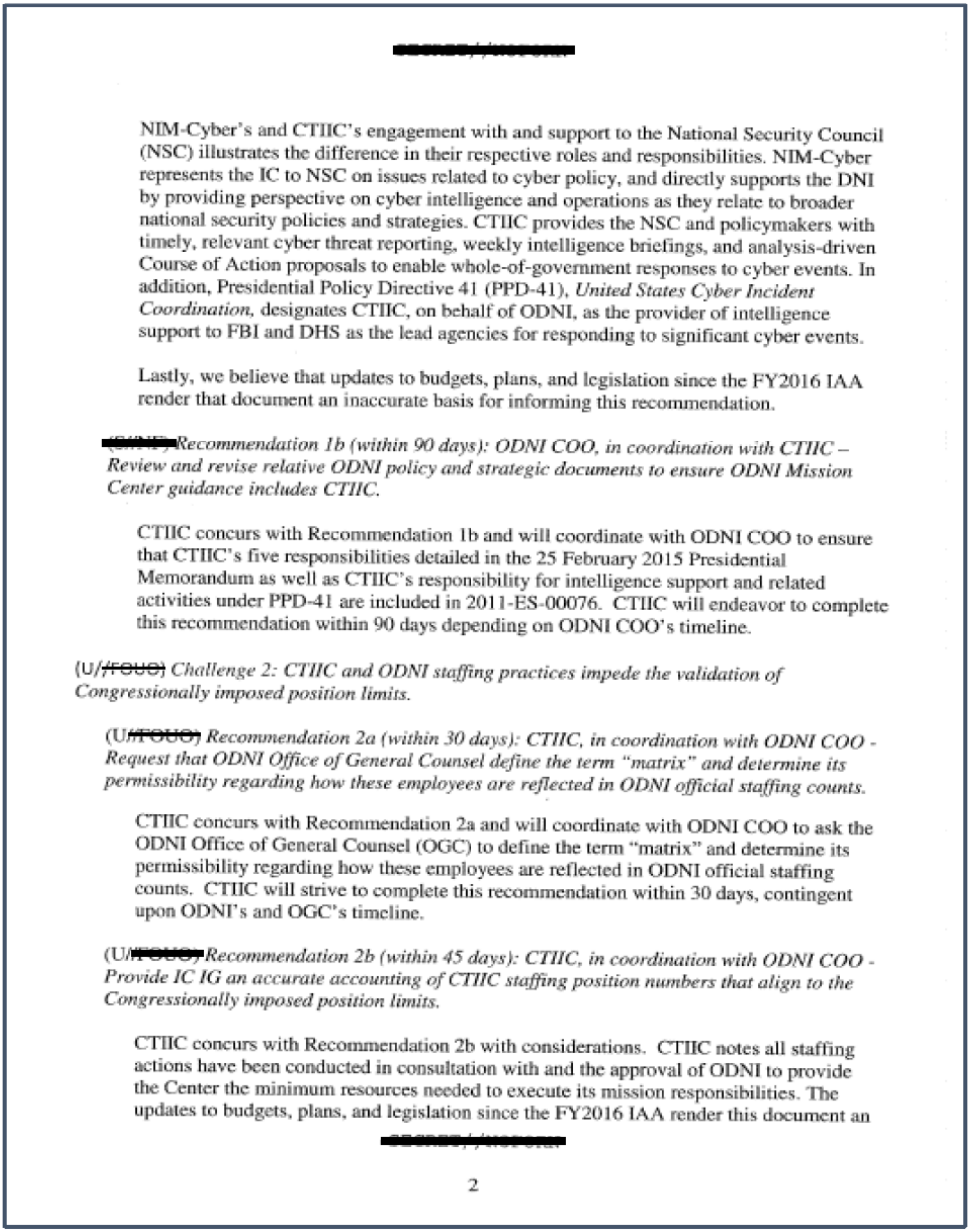
(U) *Challenge 1: The functions of the National Intelligence Manager for Cyber and CTIIC are not fully consolidated.*

~~(S//NF)~~ *Recommendation 1a (within 90 days): CTIIC, in coordination with ODNI leadership - Develop and implement a plan to combine all cyber activities, both administratively and functionally, to achieve full integration of cyber intelligence activities, as directed in the FY 2016 IAA.*

CTIIC does not concur with Recommendation 1a because it is inconsistent with previously stated ODNI leadership intent, which has been further reinforced by recent alignment of NIM-Cyber and CTIIC as a part of the ODNI-wide Transformation activities, and with the mission functions and resource needs of NIM-Cyber and CTIIC.

NIM-Cyber and CTIIC are separate functional organizations fulfilling separate and complementary activities. The NIM provides broad facilitation, guidance, and oversight of the full spectrum of Intelligence Community cyber activities – such as standards for and direction on collection, analytic focus, reporting, and community resource use and prioritization–but does not conduct analysis or publish intelligence products. CTIIC, on the other hand, conducts intelligence analysis and produces cyber threat intelligence assessments, in accordance with ODNI guidance and standards. CTIIC facilitates IC adoption of NIM-Cyber standards, such as the Cyber Threat Framework, by incorporating them into analytic production CTIIC leads on behalf of the Intelligence Community. CTIIC does not formulate policy, nor set formal community standards, and has no role in formulating community resource guidance.

[redacted]



NIM-Cyber's and CTIIC's engagement with and support to the National Security Council (NSC) illustrates the difference in their respective roles and responsibilities. NIM-Cyber represents the IC to NSC on issues related to cyber policy, and directly supports the DNI by providing perspective on cyber intelligence and operations as they relate to broader national security policies and strategies. CTIIC provides the NSC and policymakers with timely, relevant cyber threat reporting, weekly intelligence briefings, and analysis-driven Course of Action proposals to enable whole-of-government responses to cyber events. In addition, Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination,* designates CTIIC, on behalf of ODNI, as the provider of intelligence support to FBI and DHS as the lead agencies for responding to significant cyber events.

Lastly, we believe that updates to budgets, plans, and legislation since the FY2016 IAA render that document an inaccurate basis for informing this recommendation.

[redacted] *Recommendation 1b (within 90 days): ODNI COO, in coordination with CTIIC – Review and revise relative ODNI policy and strategic documents to ensure ODNI Mission Center guidance includes CTIIC.*

CTIIC concurs with Recommendation 1b and will coordinate with ODNI COO to ensure that CTIIC's five responsibilities detailed in the 25 February 2015 Presidential Memorandum as well as CTIIC's responsibility for intelligence support and related activities under PPD-41 are included in 2011-ES-00076. CTIIC will endeavor to complete this recommendation within 90 days depending on ODNI COO's timeline.

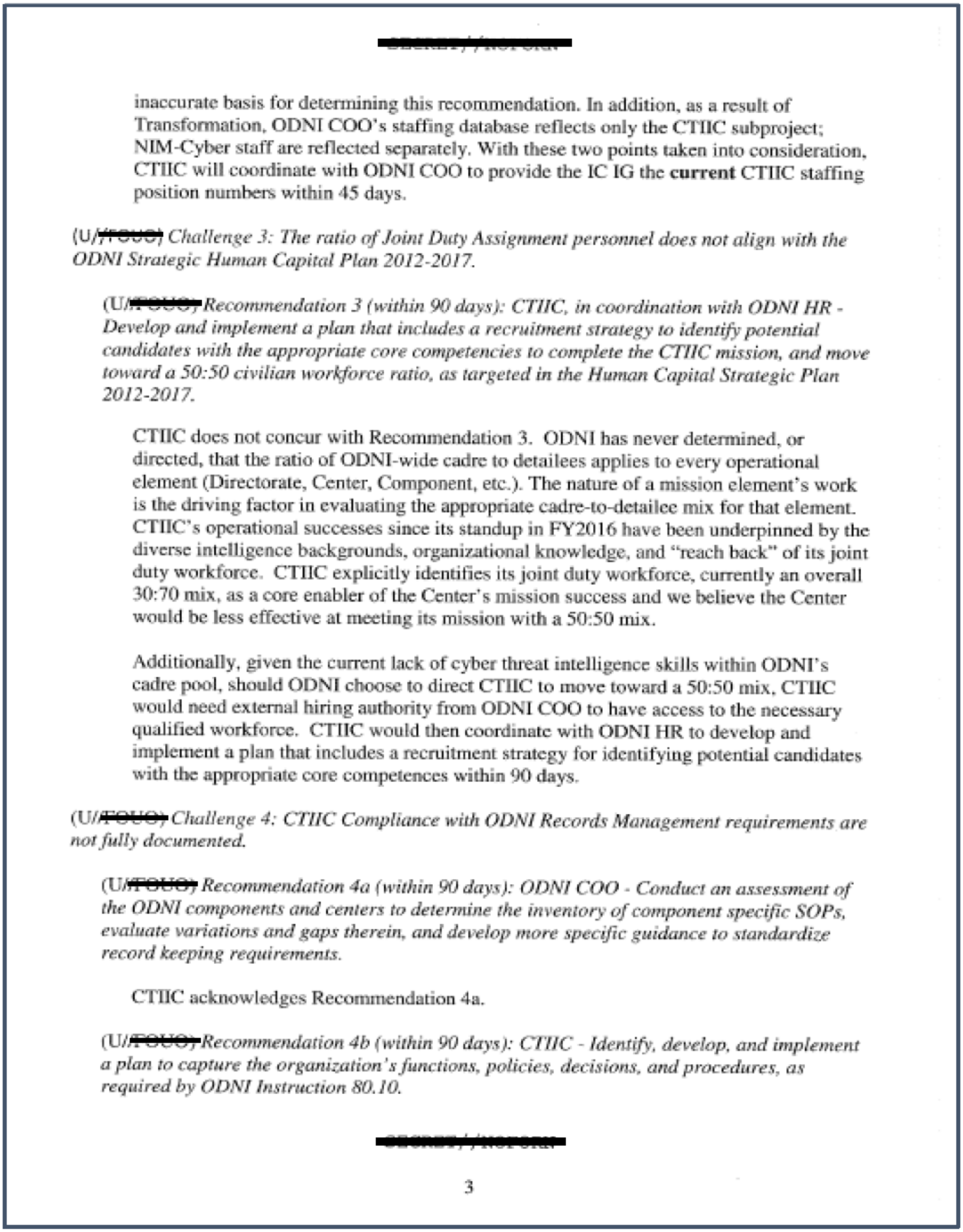
(U/~~FOUO~~) *Challenge 2: CTIIC and ODNI staffing practices impede the validation of Congressionally imposed position limits.*

(U/~~FOUO~~) *Recommendation 2a (within 30 days): CTIIC, in coordination with ODNI COO - Request that ODNI Office of General Counsel define the term "matrix" and determine its permissibility regarding how these employees are reflected in ODNI official staffing counts.*

CTIIC concurs with Recommendation 2a and will coordinate with ODNI COO to ask the ODNI Office of General Counsel (OGC) to define the term "matrix" and determine its permissibility regarding how these employees are reflected in ODNI official staffing counts. CTIIC will strive to complete this recommendation within 30 days, contingent upon ODNI's and OGC's timeline.

(U/[redacted]) *Recommendation 2b (within 45 days): CTIIC, in coordination with ODNI COO - Provide IC IG an accurate accounting of CTIIC staffing position numbers that align to the Congressionally imposed position limits.*

CTIIC concurs with Recommendation 2b with considerations. CTIIC notes all staffing actions have been conducted in consultation with and the approval of ODNI to provide the Center the minimum resources needed to execute its mission responsibilities. The updates to budgets, plans, and legislation since the FY2016 IAA render this document an



inaccurate basis for determining this recommendation. In addition, as a result of Transformation, ODNI COO's staffing database reflects only the CTIIC subproject; NIM-Cyber staff are reflected separately. With these two points taken into consideration, CTIIC will coordinate with ODNI COO to provide the IC IG the **current** CTIIC staffing position numbers within 45 days.

(U/~~/FOUO)~~ *Challenge 3: The ratio of Joint Duty Assignment personnel does not align with the ODNI Strategic Human Capital Plan 2012-2017.*

(U/~~/FOUO)~~ *Recommendation 3 (within 90 days): CTIIC, in coordination with ODNI HR - Develop and implement a plan that includes a recruitment strategy to identify potential candidates with the appropriate core competencies to complete the CTIIC mission, and move toward a 50:50 civilian workforce ratio, as targeted in the Human Capital Strategic Plan 2012-2017.*

CTIIC does not concur with Recommendation 3. ODNI has never determined, or directed, that the ratio of ODNI-wide cadre to detailees applies to every operational element (Directorate, Center, Component, etc.). The nature of a mission element's work is the driving factor in evaluating the appropriate cadre-to-detailee mix for that element. CTIIC's operational successes since its standup in FY2016 have been underpinned by the diverse intelligence backgrounds, organizational knowledge, and "reach back" of its joint duty workforce. CTIIC explicitly identifies its joint duty workforce, currently an overall 30:70 mix, as a core enabler of the Center's mission success and we believe the Center would be less effective at meeting its mission with a 50:50 mix.

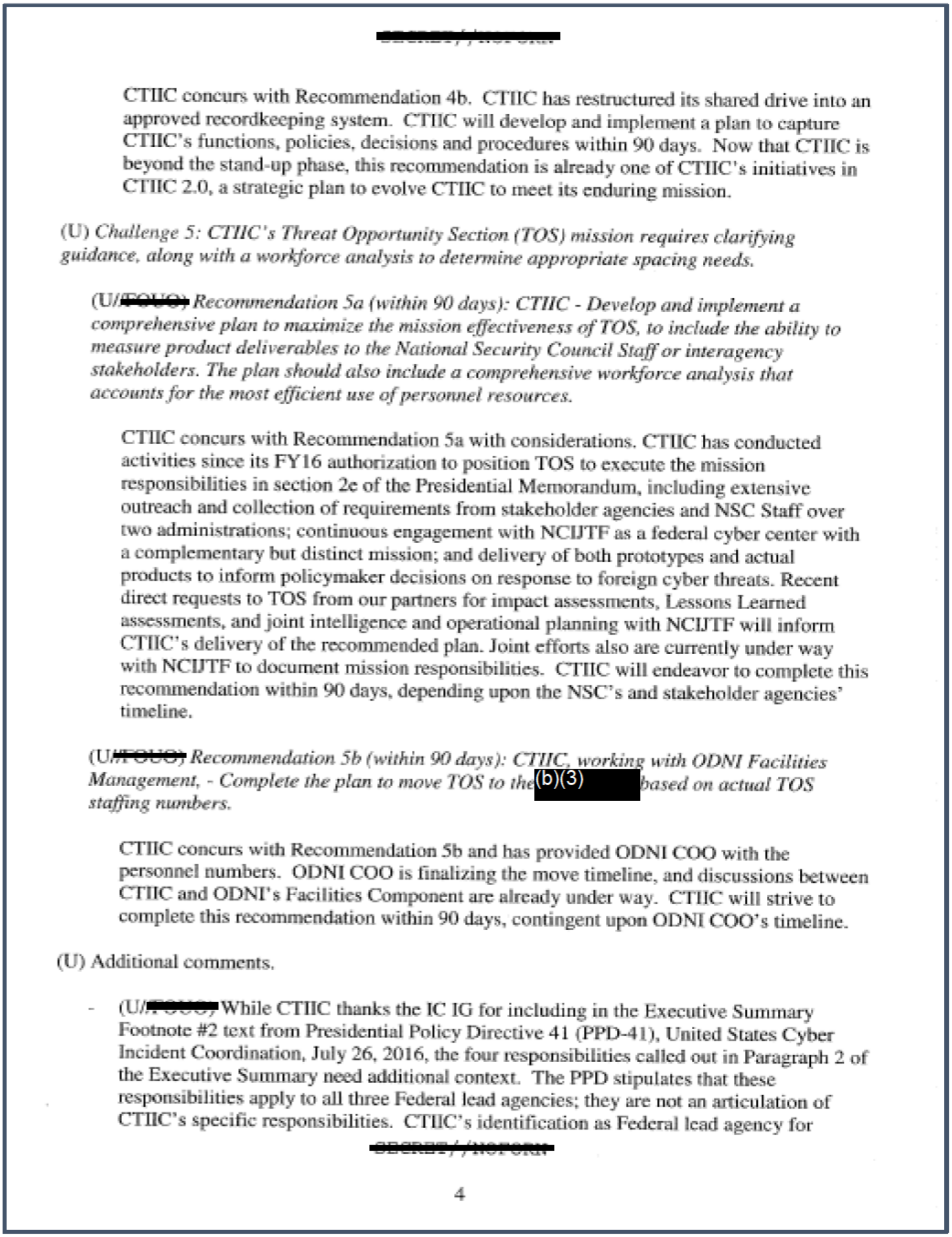
Additionally, given the current lack of cyber threat intelligence skills within ODNI's cadre pool, should ODNI choose to direct CTIIC to move toward a 50:50 mix, CTIIC would need external hiring authority from ODNI COO to have access to the necessary qualified workforce. CTIIC would then coordinate with ODNI HR to develop and implement a plan that includes a recruitment strategy for identifying potential candidates with the appropriate core competences within 90 days.

(U/~~/FOUO)~~ *Challenge 4: CTIIC Compliance with ODNI Records Management requirements are not fully documented.*

(U/~~/FOUO)~~ *Recommendation 4a (within 90 days): ODNI COO - Conduct an assessment of the ODNI components and centers to determine the inventory of component specific SOPs, evaluate variations and gaps therein, and develop more specific guidance to standardize record keeping requirements.*

CTIIC acknowledges Recommendation 4a.

(U/~~/FOUO)~~ *Recommendation 4b (within 90 days): CTIIC - Identify, develop, and implement a plan to capture the organization's functions, policies, decisions, and procedures, as required by ODNI Instruction 80.10.*



[redacted]

CTIIC concurs with Recommendation 4b. CTIIC has restructured its shared drive into an approved recordkeeping system. CTIIC will develop and implement a plan to capture CTIIC's functions, policies, decisions and procedures within 90 days. Now that CTIIC is beyond the stand-up phase, this recommendation is already one of CTIIC's initiatives in CTIIC 2.0, a strategic plan to evolve CTIIC to meet its enduring mission.

(U) *Challenge 5: CTIIC's Threat Opportunity Section (TOS) mission requires clarifying guidance, along with a workforce analysis to determine appropriate spacing needs.*

(U/[redacted] *Recommendation 5a (within 90 days): CTIIC - Develop and implement a comprehensive plan to maximize the mission effectiveness of TOS, to include the ability to measure product deliverables to the National Security Council Staff or interagency stakeholders. The plan should also include a comprehensive workforce analysis that accounts for the most efficient use of personnel resources.*

CTIIC concurs with Recommendation 5a with considerations. CTIIC has conducted activities since its FY16 authorization to position TOS to execute the mission responsibilities in section 2e of the Presidential Memorandum, including extensive outreach and collection of requirements from stakeholder agencies and NSC Staff over two administrations; continuous engagement with NCIJTF as a federal cyber center with a complementary but distinct mission; and delivery of both prototypes and actual products to inform policymaker decisions on response to foreign cyber threats. Recent direct requests to TOS from our partners for impact assessments, Lessons Learned assessments, and joint intelligence and operational planning with NCIJTF will inform CTIIC's delivery of the recommended plan. Joint efforts also are currently under way with NCIJTF to document mission responsibilities. CTIIC will endeavor to complete this recommendation within 90 days, depending upon the NSC's and stakeholder agencies' timeline.

(U[redacted] *Recommendation 5b (within 90 days): CTIIC, working with ODNI Facilities Management, - Complete the plan to move TOS to the* (b)(3) *based on actual TOS staffing numbers.*

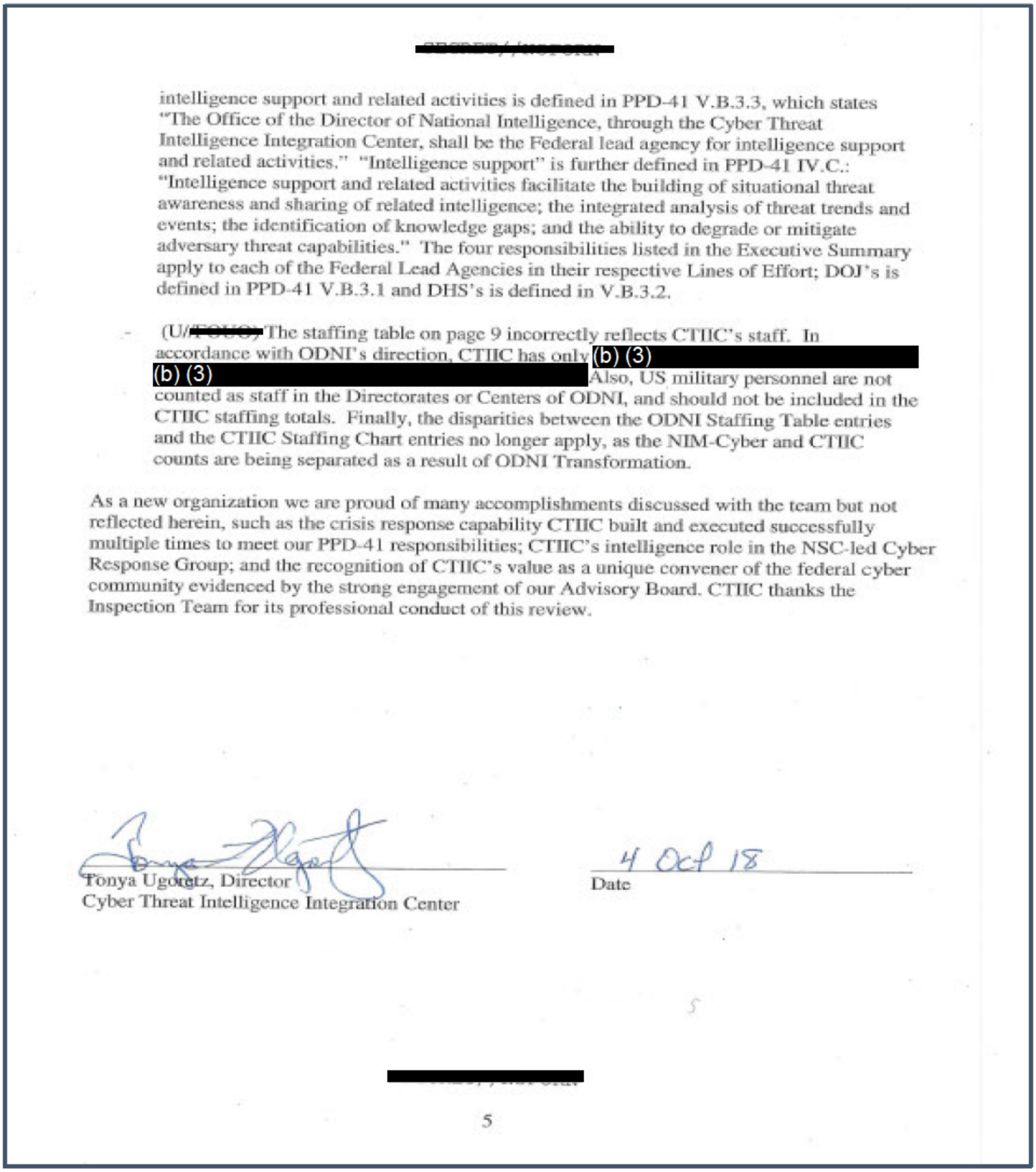
CTIIC concurs with Recommendation 5b and has provided ODNI COO with the personnel numbers. ODNI COO is finalizing the move timeline, and discussions between CTIIC and ODNI's Facilities Component are already under way. CTIIC will strive to complete this recommendation within 90 days, contingent upon ODNI COO's timeline.

(U) Additional comments.

- (U/[redacted] While CTIIC thanks the IC IG for including in the Executive Summary Footnote #2 text from Presidential Policy Directive 41 (PPD-41), United States Cyber Incident Coordination, July 26, 2016, the four responsibilities called out in Paragraph 2 of the Executive Summary need additional context. The PPD stipulates that these responsibilities apply to all three Federal lead agencies; they are not an articulation of CTIIC's specific responsibilities. CTIIC's identification as Federal lead agency for

[redacted]

4



intelligence support and related activities is defined in PPD-41 V.B.3.3, which states "The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, shall be the Federal lead agency for intelligence support and related activities." "Intelligence support" is further defined in PPD-41 IV.C.: "Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities." The four responsibilities listed in the Executive Summary apply to each of the Federal Lead Agencies in their respective Lines of Effort; DOJ's is defined in PPD-41 V.B.3.1 and DHS's is defined in V.B.3.2.

- (U/[redacted] The staffing table on page 9 incorrectly reflects CTIIC's staff. In accordance with ODNI's direction, CTIIC has only (b) (3) (b) (3) Also, US military personnel are not counted as staff in the Directorates or Centers of ODNI, and should not be included in the CTIIC staffing totals. Finally, the disparities between the ODNI Staffing Table entries and the CTIIC Staffing Chart entries no longer apply, as the NIM-Cyber and CTIIC counts are being separated as a result of ODNI Transformation.

As a new organization we are proud of many accomplishments discussed with the team but not reflected herein, such as the crisis response capability CTIIC built and executed successfully multiple times to meet our PPD-41 responsibilities; CTIIC's intelligence role in the NSC-led Cyber Response Group; and the recognition of CTIIC's value as a unique convener of the federal cyber community evidenced by the strong engagement of our Advisory Board. CTIIC thanks the Inspection Team for its professional conduct of this review.

Tonya Ugoretz, Director
Cyber Threat Intelligence Integration Center

4 Oct 18
Date

(U) Appendix H: ICIG Response to CTIIC Comments

(U) Challenge 1: The functions of the National Intelligence Manager for Cyber and CTIIC are not fully consolidated.

~~(S//NF)~~ **Recommendation 1a (within 90 days):** CTIIC, in coordination with ODNI leadership – Develop and implement a plan to combine all cyber activities, both administratively and functionally, to achieve full integration of cyber intelligence activities, as directed in the FY 2016 IAA.

(U) CTIIC Response:

(U/~~/FOUO)~~ CTIIC does not concur with Recommendation 1a because it is inconsistent with previously stated ODNI leadership intent, which has been further reinforced by recent alignment of NIM-Cyber and CTIIC as a part of the ODNI-wide Transformation activities, and with the mission functions and resource needs of NIM-Cyber and CTIIC.

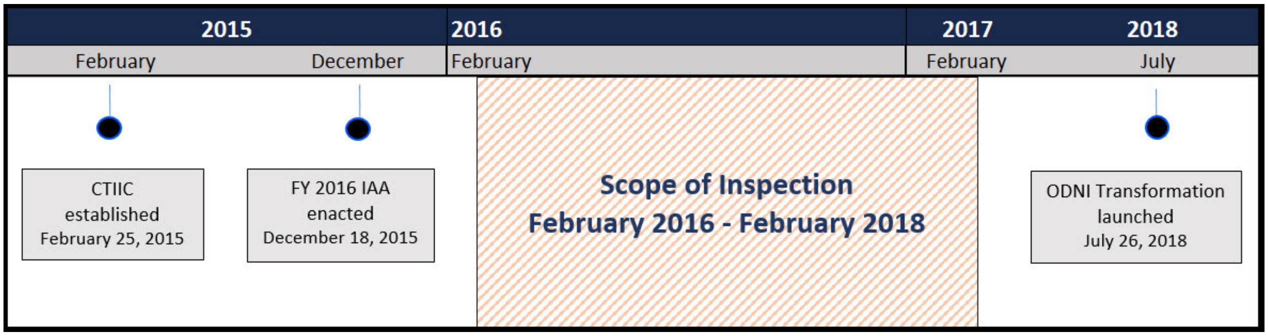
(U/~~/FOUO)~~ NIM-Cyber and CTIIC are separate functional organizations fulfilling separate and complementary activities. The NIM provides broad facilitation, guidance, and oversight of the full spectrum of Intelligence Community cyber activities – such as standards for and direction on collection, analytic focus, reporting, and community resource use and prioritization-but does not conduct analysis or publish intelligence products. CTIIC, on the other hand, conducts intelligence analysis and produces cyber threat intelligence assessments, in accordance with ODNI guidance and standards. CTIIC facilitates IC adoption of NIM-Cyber standards, such as the Cyber Threat Framework, by incorporating them into analytic production CTIIC leads on behalf of the Intelligence Community. CTIIC does not formulate policy, nor set formal community standards, and has no role in formulating community resource guidance.

((U/~~/FOUO)~~ NIM-Cyber's and CTIIC's engagement with and support to the National Security Council (NSC) illustrates the difference in their respective roles and responsibilities. NIM-Cyber represents the IC to NSC on issues related to cyber policy, and directly supports the DNI by providing perspective on cyber intelligence and operations as they relate to broader national security policies and strategies. CTIIC provides the NSC and policymakers with timely, relevant cyber threat reporting, weekly intelligence briefings, and analysis-driven Course of Action proposals to enable whole-of-government responses to cyber events. In addition, Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, designates CTIIC, on behalf of ODNI, as the provider of intelligence support to FBI and DHS as the lead agencies for responding to significant cyber events.

(U/~~/FOUO)~~ Lastly, we believe that updates to budgets, plans, and legislation since the FY 2016 IAA render that document an inaccurate basis for informing this recommendation.

(U) ICIG Response:

~~(S//NF)~~ ODNI's leadership intent does not negate, replace, or modify the law. The congressional requirement to consolidate the functions of NIM-Cyber with those of CTIIC has been in effect since December 18, 2015. To date, ODNI has not complied with that legal requirement. Indeed, contrary to law, CTIIC's response states that "NIM-Cyber and CTIIC are *separate functional* organizations." The ICIG acknowledges ODNI's ongoing transformational activities, and in time these efforts may achieve and comply with CTIIC's obligations under the FY 2016 IAA, if that is an intended purpose or an incidental consequence of the transformation. However, the transformational activities post-date the fieldwork of this inspection, and were not assessed during the course of this inspection. In the meantime, CTIIC's response has raised a serious concern for the ICIG because the response suggests that CTIIC believes it is not required to comply with – and has no present intention of complying with – the legal requirements set forth in the FY 2016 IAA. Until such time as ODNI's actions achieve the results required in the IAA, our Recommendation remains necessary and supportable.


2015
2016
2017
2018
February
December
February
February
July
CTIIC established February 25, 2015
FY 2016 IAA enacted December 18, 2015
Scope of Inspection February 2016 - February 2018
ODNI Transformation launched July 26, 2018

(U/~~/FOUO)~~ Recommendation 2b: CTIIC, in coordination with ODNI COO - Provide ICIG an accurate accounting of CTIIC staffing position numbers that align to the congressionally imposed position limits.

(U) CTIIC Response:

(U/~~/FOUO)~~ CTIIC concurs with Recommendation 2b with considerations. CTIIC notes all staffing actions have been conducted in consultation with and the approval of ODNI to provide the Center the minimum resources needed to execute its mission responsibilities. The updates to budget, plans, and legislation since the FY 2016 IAA render this document an inaccurate basis for determining this recommendation. In addition, as a result of transformation, ODNI COO's staffing database reflects only the CTIIC subproject: NIM-Cyber staff are reflected separately.

With these two points taken into consideration, CTIIC will coordinate with ODNI COO to provide the ICIG the current CTIIC staffing position numbers within 45 days.

(U) ICIG Response:

(U) While CTIIC notes that staffing actions may have been conducted in consultation with the ODNI, as previously stated, ICIG is not aware of any legislation that negated, replaced, or modified the FY 2016 IAA. Moreover, updates to budgets and plans do not negate, replace, or modify the law.

(U) Challenge 3: The ratio of Joint Duty Assignment personnel does not align with the ODNI *Strategic Human Capital Plan 2012-2017*.

(U/~~/FOUO)~~ Recommendation 3 (within 90 days): CTIIC, in coordination with ODNI HR – Develop and implement a plan that includes a recruitment strategy to identify potential candidates with the appropriate core competencies to complete the CTIIC mission, and move toward a 50:50 civilian workforce ratio, as targeted in the *Strategic Human Capital Plan 2012-2017*.

(U) CTIIC Response:

(U/~~/FOUO)~~ CTIIC does not concur with Recommendation 3. ODNI has never determined, or directed, that the ratio of ODNI-wide cadre to detailees applies to every operational element (Directorate, Center, Component, etc.). The nature of a mission element's work is the driving factor in evaluating the appropriate cadre-to-detailee mix for that element. CTIIC's operational successes since its standup in FY 2016 have been underpinned by the diverse intelligence backgrounds, organizational knowledge, and "reach back" of its joint duty workforce. CTIIC explicitly identifies its joint duty workforce, currently an overall 30:70 mix, as a core enabler of the Center's mission success and we believe the Center would be less effective at meeting its mission with a 50:50 mix.

(U/~~/FOUO)~~ Additionally, given the current lack of cyber threat intelligence skills within ODNI's cadre pool, should ODNI choose to direct CTIIC to move toward a 50:50 mix, CTIIC would need external hiring authority from ODNI COO to have access to the necessary qualified workforce. CTIIC would then coordinate with ODNI HR to develop and implement a plan that includes a recruitment strategy for identifying potential candidates with the appropriate core competences within 90 days.

(U) ICIG Response:

(U) There was no evidence that CTIIC requested or received an exemption from the goal of moving toward a 50:50 cadre to JDA ratio. The ODNI *Strategic Human Capital Plan 2012-2017* recognizes that one of the most significant challenges in standing up a new organization is staffing it with personnel who have the necessary core competencies. The Plan calls for a total workforce approach that will work toward a 50:50 ODNI cadre to JDA ratio to help build a more collaborative, agile, and knowledgeable workforce.

(U) The ICIG acknowledges that recruiting personnel with the appropriate cyber skills may be difficult for CTIIC. However, each of the other three ODNI Mission Centers, with their own distinctive personnel requirements, have proven capable of moving toward a closer mix of 50:50 cadre to JDA ratio. CTIIC, now in its fourth year of existence, should be able to formulate an executable plan of action towards the desired workforce mix while ensuring staff have the core competencies necessary to complete the CTIIC mission. Regardless, CTIIC's response has raised a serious concern for the ICIG because the response suggests that CTIIC believes it is not required to comply with – and has no present intention of complying with – the goal of moving toward a 50:50 cadre to JDA ratio.

(U) CTIIC's Additional Comments:

(U/~~/FOUO)~~ The Staffing Table on page 9 incorrectly reflects CTIIC's staff. In accordance with ODNI's direction, CTIIC only has (b)(3) (b)(3) Also, U.S. military personnel are not counted as staff in the Directorates or Centers of ODNI, and should not be included in the CTIIC staffing totals. Finally, the disparities between the ODNI Staffing Table entries and the CTIIC Staffing Chart entries no longer apply, as the NIM-Cyber and CTIIC counts are being separated as a result of ODNI Transformation.

(U) ICIG Response:

(U/~~/FOUO)~~ During the initial data call request, CTIIC provided the ICIG with a detailed staffing chart to assist with our review. The provided staffing chart reflected (b)(3) (b)(3) Furthermore, as stated on page 9, paragraph 4 of the CTIIC Inspection Report, Table 1 evidences the inconsistencies in staff position counts for the scope of our review, February 2016 – February 2018. The ICIG remains concerned that CTIIC and ODNI staffing practices impede the validation of congressionally imposed position limits.

Inspector General of the Intelligence Community

Integrity, Professionalism, Independence

Hotline: 933-2800 (secure) or 1-855-731-3260 (open)