United States Cyber Command
Joint Force Headquarters-DODIN

FY20 NDAA Sec 1645 Report: Cyber Attacks and Intrusions against the Department of Defense by Certain Foreign Entities

Reporting Period: 01APR19-31MAR20

(U//~~FOUO~~) Background: Section 1645 of the National Defense Authorization Act (NDAA) for Fiscal Year 2020 requires the Department of Defense (DOD) to submit a report on cyber-attacks and intrusions over the previous 12 months by agents or associates of the Governments of the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, and the Democratic People's Republic of Korea against: the DOD; DOD contractors working on sensitive United States military technology; and the personal communications of the personnel of the DOD. [1] Joint Force Headquarters – Department of Defense Information Network (JFHQ-DODIN) is a USCYBERCOM headquarters, responsible for the global Command and Control (C2) of all DODIN Operations and Defensive Cyberspace Operations, Internal Defensive Measures (DCO-IDM), to include the DOD's unclassified and classified networks and information systems.[2] This report will address foreign cyberspace attacks and intrusions into DOD owned, leased or operated systems and networks only, as our DCSA and DC3 partners can address activity impacting DOD cleared defense contractor (CDC) systems, networks or information.

(U//~~FOUO~~) The DOD Information Network (DODIN): The DODIN encompasses all communications and computing systems, services, software, data, security services, and national security systems owned or leased by the DOD.[3] [redacted]

(U) FISA NOTICE: This document contains information that is Foreign Intelligence Surveillance Act (FISA) derived. Per 50 U.S.C. Section 1806(b), recipients are reminded that this information, or any information derived from it, may only be used in a criminal proceeding with the advanced authorization of the Attorney General. This information may not be disseminated to a foreign government without the authorization of the Attorney General. Any reproduction of this information must be accompanied by a statement of these restrictions.

(b)(3) 10 U.S.C. §130e
(b)(3) 50 U.S.C. §3024(i)(1)

(U) Definition of Attack and Intrusion: For the purpose of this report, we are defining "attacks" as malicious activity, (known or suspected to have been) conducted by one of the nation-states of concern, directed against the DODIN. Examples of attacks include reconnaissance, vulnerability scanning, phishing, denial of service and access attempts. We are defining "intrusions" as successful adversary activity that resulted in host or system compromise, unauthorized system access or data exfiltration.

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

[redacted]

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

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

(b)(3) 10 U.S.C. §130e
(b)(3) 50 U.S.C. §3024(i)(1)

[A] "A Day in the Life of the DODIN," Slide, DISA, Undated

(b)(3) 10 U.S.C. §130e
(b)(3) 50 U.S.C. §3024(i)(1)

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

(~~S//NF~~) Incident Reporting: [redacted]

(U) Analysis of Intelligence and Incident Reporting:

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

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

[redacted]

(b)(3) 50 U.S.C. §3024(i)(1)

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

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

[redacted]

(U) Targeting of the Personal Communications of the Personnel of the Department of Defense:

(U) The section below attempts to answer part three of the NDAA tasker with regard to targeting of personal communications of DOD personnel.

[redacted]

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

[redacted]

(U/~~/FOUO~~) *This report includes the results of closed investigations, where the intelligence community reporting provided reasonable certainty of attribution. JFHQ-DODIN did not include data from open investigations where analysts have been unable to determine attribution based on currently available information.* [redacted] *JFHQ-DODIN will include such data in the next report if subsequent investigation allows for attribution of these incidents.*

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

(b)(3) 50 U.S.C. §3024(i)(1)

TAB A
DOD Internet Access Points (IAPs)

[redacted]

(b)(3) 50 U.S.C. §3024(i)(1)

TAB B
DOD Information Network Areas of Operation (AOs)

[redacted]

(b)(3) 50 U.S.C. §3024(i)(1)

(b)(3) 50 U.S.C. §3024(i)(1)

[1] (U) SEC. 1645. ANNUAL REPORT ON CYBER ATTACKS AND INTRUSIONS AGAINST THE DEPARTMENT OF DEFENSE BY CERTAIN FOREIGN ENTITIES.

(a) In General.—Not later than 180 days after the date of the enactment of this Act, and each fiscal year thereafter through fiscal year 2023, the Secretary of Defense shall submit to the congressional defense committees a report on cyber-attacks and intrusions in the previous 12 months by agents or associates of the Governments of the Russian Federation, the People's Republic of China, the Islamic Republic of Iran, and the Democratic People's Republic of Korea against or into—

(1) the information systems (as such term is defined in section 3502 of title 44, United States Code) of—

(A) the Department of Defense; and

(B) any contractor of the Department of Defense that works on sensitive United States military technology; and

(2) the personal communications of the personnel of the Department of Defense.

(b) Form.—The report required by subsection (a) shall be submitted in classified form.

[2] (U) EXORD TO IMPLEMENT UPDATED CYBERSPACE OPERATIONS COMMAND AND CONTROL (C2) FRAMEWORK (S//REL TO USA, FVEY), dated 1 FEB 2016

[3] (U) Joint Publication 3-12, Cyberspace Operations, dated 8 JUN 2018.

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

[5] (U) See Tab B, DOD Areas of Operation (AOs)

[6] (U) See Tab A, DOD Internet Access Points

[7] (U) Department of Defense Information Network 2019 Operational Risk Assessment, JFHQ-DODIN, dated 31 JUL 2020

[8] (U) Data is derived from analysis of [redacted]

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

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

[11] (U) [redacted]

[12] (U) The Joint Incident Management System (JIMS) is the designated DOD central cyber incident reporting registry as designated in CJCSM 6510.01B, Cyber Incident Handling Program, 18 DEC 2014

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

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

[15] (U) Joint Statement by the Directors of the Intelligence Community, January 2017

[16] (U) STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY, ODNI, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

[17] (U) Department of Defense Information Network 2019 Operational Risk Assessment, JFHQ-DODIN, 31 JUL 2020

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

[19] Open Source Research / Collection is when the adversary accesses publically available websites, including DOD, cleared defense contractor (CDC) or US Government sites to collect data related to DOD. This data can serve to fill adversary collection gaps, or can be used to refine cyber or intelligence targeting.

[20] (U) Reconnaissance / Scanning activity is when the adversary attempts to map or enumerate DOD systems / networks, determine available ports and protocols, or identify existing vulnerabilities or misconfigurations

[21] (~~S//REL TO USA, FVEY~~) [redacted]

[22] (U) Suspicious Connection are instances where anomalous activity is detected, but the exact nature of the event cannot be clearly ascertained. In this case, the activity has been linked to MCA indicators of compromise (IOCs).

[23] (U) Malicious Logic / Malware are instances where malicious scripts or code are detected by network defenses. In this case, the activity has been linked to MCA indicators of compromise (IOCs).

[24] (U) Access / Exploitation Attempts occur when attackers attempt to gain unauthorized access to DOD systems or networks using a variety of techniques, such as failed logon attempts or password attacks. In this case, the activity has been linked to MCA indicators of compromise (IOCs).

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

(b)(3) 50 U.S.C. §3024(i)(1)

[25] (U) Data is derived from analysis of [redacted]

[26] (U) STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT of the US INTELLIGENCE COMMUNITY, ODNI, January 29, 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

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

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

[29] (U) Department of Defense Information Network 2019 Operational Risk Assessment, JFHQ-DODIN, 31 JUL 2020

[30] (U) Typosquatting / Malicious Redirection utilizes techniques to force users away from legitimate domains / websites, to malicious domains / websites established by the MCA

[31] (U) Social Engineering is the exploitation of human nature to force the disclosure of sensitive information, or to entice the user to conduct an action that benefits the attacker. These activities can be conducted through email, voice, text message, social media, face to face or via other means.

[32] (U) Spearphishing / Phishing is the use of false communications, typically email, to entice a user to conduct an action, or disclose sensitive information. Phishing is generally widespread, whereas spearphishing is typically tailored and targeted.

[33] (U) Data is derived from analysis of [redacted]

[34] (U) Department of Defense Information Network 2019 Operational Risk Assessment, JFHQ-DODIN, dated 31 JUL 2020

[35] (U) Malicious URL / File Downloads occur when a user accesses a malicious URL, or site, or downloads a malicious file. In this case, the activity has been linked to MCA indicators of compromise (IOCs).

[36] (U) Data is derived from analysis of [redacted]

[37] (U) [redacted]

[38] (U) Appendix 11 to Annex B to OGS-17, JFHQ-DODIN, 3 August 2017

[39] (U) Department of Defense Information Network 2019 Operational Risk Assessment, JFHQ-DODIN, 31 JUL 2020

[40] (U) Credential Harvesting utilizes a variety of techniques to capture user credentials (i.e. user names and passwords) in order to access targeted systems at a later time. In this case, the activity has been linked to MCA indicators of compromise (IOCs).

[41] (U) Data is derived from analysis of [redacted]

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

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

[44] [redacted]

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

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

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

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

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

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

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

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

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

(b)(3) 50 U.S.C. §3024(i)(1)

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

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

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

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

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

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

[59] (~~S//REL TO USA, FVEY~~) [redacted]

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

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

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

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

[64] (U) [redacted]

[65] (~~S//REL TO USA, FVEY~~) [redacted]

[66] (~~S//REL TO USA, FVEY/FISA~~) [redacted]

[67] (~~S//REL TO USA, FVEY/FISA~~) [redacted]

[68] (~~S//REL TO USA, FVEY/FISA~~) [redacted]

[69] (U) [redacted]

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

JFHQ-DODIN POC:

[redacted] (b)(6)

(b)(3) 50 U.S.C. §3024(i)(1)

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

UNITED STATES CYBER COMMAND

(USCYBERCOM)

Section 1635 Report on USCYBERCOM Acquisition Authority

October 2018

Background: Section 1635 of the Fiscal Year 2019 National Defense Authorization Act Joint Explanatory Statement requires the Commander, U.S. Cyber Command (USCYBERCOM), to produce a report detailing the use of the command's $75M acquisition authority. The requested report must also include the following:

- An assessment of any impacts of the expenditure limit set on the exercise of this authority on planned Cyber Command acquisition activities, as well as a juxtaposition of the types of cyber-peculiar products, services, and technologies procured using this authority and those cyber capabilities procured by the Services using their acquisition authorities.
- Definition of cyber-peculiar capabilities and cyber-peculiar services, a description of memoranda of agreements with the Services for acquisition of cyber capabilities and details regarding the acquisition expertise at U.S. Cyber Command, including the number of senior acquisition executives and contracting officials authorized to be hired at the headquarters.

FY18 Use of the Command's $75M Acquisition Authority

In FY18, USCYBERCOM started the transition from an organization relying primarily on leveraging the contracts of our military Service and agency partners to establishing contracts leveraging our current authority. In FY18, the command executed 32 contract actions totaling $43M versus the award of a single contract in FY17 totaling $900K. Execution of our current authorities has allowed the command to provide faster responses to urgent Cyber Mission Force (CMF) needs, move prototype efforts such as Unified Platform (UP) and Joint Cyber Command and Control (JCC2) forward and put the initial contracting foundation in place for future support. Key efforts included implementation of cloud and engineering services in support of a big data platform, foundational pieces of the architecture for implementation of continuous monitoring, a Partnership Intermediary Agreement (PIA) for unclassified innovation, and a competitive cyber tool contract.

Command requirements and planned contracting activities for FY19 will continue the upward trend in leveraging our current authorities to continue building the foundation of both base contracts and skilled personnel to increase execution. Our current projections indicate we will execute between $60M – $75M in FY19.

Assessment of expenditure limit impacts:

FY18 – No impact – Personnel bandwidth limited our ability to approach our current ceiling. The increase of the sunset date in FY19 has helped with our implementation of multi-year awards and our messaging to the vendor community.
(~~FOUO~~) FY19 – Limited impact – With continued building of our acquisition/contracting expertise, we expect the use of our authorities to get within reach of the ceiling limit. Our vendor base is very much aware of the caps in our authorities limiting interest in creating partnerships as we pursue innovative technologies for CMF needs.

(~~FOUO~~) Overall impact – Limiting spending authority leaves the command to rely on the contract vehicles of the military Services or agencies – significantly hampering our ability to properly manage obligation and outlay rates in pursuit of DoD goals. Matching existing contract scope from our partners has proved difficult requiring the command to modify requirements, look for other vehicles, or wait until the partner can award a new task order – adding months to the delivery timeframe and in turn, reducing the command's ability to rapidly procure needed capabilities to support the Cyber Mission Force.

Juxtaposition between CDG and Services:

Services are executing enterprise-wide programs whereas USCYBERCOM is executing smaller efforts based on Cyber Requirements Evaluation Board (CREB) validated requirements. The Services are responsible for the Unified Platform (UP), Persistent Cyber Training Environment (PCTE), and Joint Cyber Command and Control (JCC2) programs, which are all considered programs of record. Further, the Services are authorized to acquire major defense acquisition programs, major automated information systems programs, acquisitions of foundational infrastructure, and software architectures, the duration of which is expected to last more than five years. USCYBERCOM is not authorized to perform these types of acquisitions.

Definitions (Cyber-Peculiar Capabilities (CPC) and Cyber-Peculiar Services (CPS))

Background: The nature of cyberspace, cyberspace operations (CO) and their relationship with cyber-peculiar capabilities (CPC) and cyber-peculiar services (CPS) can be categorized as mutually dependent. CO rely on networked, stand-alone, and platform–embedded IT infrastructure, in addition to the data that reside on and are transmitted through these components to enable military operations in a man-made domain.

Definition: Cyber-peculiar capabilities and services are defined as any acquisition effort that supports or facilitates any of the three Cyberspace Missions as defined in Joint Pub 3-12 – "Offensive Cyber Operations, Defensive Cyber Operations, or Department of Defense Information Network operation. These three mission types comprehensively cover the activities of the cyberspace forces."

Memoranda of Agreement:

Currently, Memoranda of agreement are in place between USCYBERCOM and NSA (Limited Financial and Acquisition Support), USSOCOM (Small Business Advisor Support), and the 11th Wing (Air Force District Washington (AFDW) – Base Mission Support – Finance and Gov't Purchase Card). USCYBERCOM also has two agreements in place for 2nd party partner development efforts (United Kingdom, Australia).

Number of Senior Acquisition Executives and Contracting officials authorized at Headquarters:

Currently, the Command is authorized one senior-level (SES) Component Acquisition Executive (CAE), one Head of Contracting Activity (HCA) at the GG-15 level, and two contracting specialists. The current acting CAE is Defense Acquisition Workforce Improvement Act (DAWIA)-level-3-certified and has over 25 years acquisition experience. The current HCA is DAWIA-level-3-certified, holds an unlimited warrant and has 15 years' experience.

(~~FOUO~~) In 2016, the Joint Manning Validation Boards validated 40 acquisition billets for the Capabilities Development Group. However, only 10 of the 40 were resourced and of those 10, only three (3) are contracting billets; these billets include the HCA and two contract specialists. The HCA and one specialist are onboarding in Oct 2018. The second specialist is expected by 2QFY19. To fill the gap, the command has requested, and received, support from the Air National Guard via the assignment of a military contracting officer (CO) to the division; currently that CO has been issued a limited warrant.

The requested increase in acquisition authority dictates the remaining seven contracting billets be resourced (bringing the total number of contracting personnel in the division to 10 to efficiently and effectively execute the command's mission requirements.

UNITED STATES CYBER COMMAND

Response to Congress

GEN Nakasone Confirmation Hearing Response to Senator King

November 2018

~~**FOR OFFICIAL USE ONLY, NOT FOR PUBLICATION OR PUBLIC RELEASE**~~

(U) **PURPOSE:**

(U) This response to Congress is intended to answer Senator King's (D-ME) question on retention posed to then-Lieutenant General Paul M. Nakasone during the 1 March 2018 Confirmation Hearing.

(U) During the confirmation hearing, Senator King asked: *"Subsequent to your confirmation, provide an analysis or report on the issues of recruitment and retention in Cyber Command. This is an area where people are the most important asset. I fear that, for a number of reasons, whether it's the slowness of the clearance process, whether it's the way the bureaucracy works, we're not going to be able to retain and recruit the crucial people that we need."*

(U) **OVERVIEW:**

(U) While recruitment and retention continue to be a main focus for United States Cyber Command (USCYBERCOM) and its Cyber Service Components, in general, there are no major issues with recruitment and retention that impact USCYBERCOM's ability to conduct its operations. The sections below provide details on both civilian and military recruitment and retention.

(U) **BACKGROUND:**

(U) **Recruitment and Retention Incentives for Civilians**

(U) As a trailblazer for the Department of Defense's (DoD) Cyber Excepted Service (CES) personnel system, USCYBERCOM CES implementation was finalized on 18 February 2018. Ultimately, 79% of USCYBERCOM Air Force civilians entered Cyber Excepted Service. CES hiring authorities are critical to recruit high-quality civilians while offering competitive compensation packages. USCYBERCOM is using new, fast and flexible hiring authorities to tackle civilian vacancies and recruit vital cyber talent.

(U) CES enables agile recruitment options. Outside the confines of the traditional Air Force civilian hiring process, USCYBERCOM is pushing past the norms of laborious, slow hiring by actively recruiting talent through job fairs and hiring events where USCYBERCOM screens resumes and conducts on-site interviews leading to the best candidates receiving job offers. USCYBERCOM is now conducting monthly hiring events with over 50 job offers presented since CES implementation. CES allows for direct hire authority and "on-the-spot" appointments. Several events use this "on-the-spot" format with interviews and job offers. For example, the Command's hiring event on 8 May resulted in 18 same-day job offers sourced from over 900 candidates attending virtually and in-person and over 70 live interviews.

(U) CES also streamlines hiring procedures enabling USCYBERCOM to quickly acquire talent. As of October 2018, the Command is seeing positive timeline improvements with the use of CES authorities. Prior to CES, the command averaged 111 days for a selected employee to receive a job offer. Following CES implementation, this average has been reduced to 44 days. This does not include the significant security vetting process which continues to challenge the Department of Defense.

(U//~~FOUO~~) As part of CES, USCYBERCOM received authorization to offer civilian recruitment incentives up to 50% of basic pay. USCYBERCOM will continue to proactively leverage the military Services to use the full extent of CES through flexible pay-setting, compensation initiatives, career roadmaps, rotational assignments and detailed training programs.

(U) Lastly, USCYBERCOM is also growing its intern programs by 300%. By recruiting the best and brightest cyber talent from the Nation's colleges and universities, the Command offers paid, three-year internships with extensive job training, professional development and rotational assignments with the goal of building tomorrow's cyber leaders and outplacing the best into permanent positions in USCYBERCOM upon completion of their program.

(U) While USCYBERCOM sees considerable improvement to recruiting, the Department has yet to implement all of the compensation incentives CES provides. The Department of Defense's Chief Information Officer (CIO) is gathering compensation analytics from each of the Services to present and implement a Targeted Local Market Supplement for highly specialized skills or hard to fill positions which will compensate talent closer to industry norms. Additionally, the Department is leading an effort as a part of the recently signed DoD Cyber Security Strategy to explore a retention bonus (25% base pay) for those who may depart DoD and build career development opportunities through internships and details with industry or academia.

(U) **Recruitment and Retention Incentives for Cyber Military Service Members**

(U) For our military workforce, like the other Combatant Commands, USCYBERCOM relies on the Services to recruit and retain the talent we need to deliver joint force objectives for the Nation. We applaud the diligent efforts of the Services to organize, train and equip cyber operations forces, including fully leveraging recruitment and retention incentives and creating talent management programs that grow a robust cyber workforce.

(U) For example, the Army created a cyber branch to identify and track Soldiers with cyber expertise for important work roles and career development. The Army expanded compensation for cyber Soldiers in difficult-to-fill work roles and enacted Special-Duty Assignment Pay for eligible enlisted cyber positions. Additionally for the Army, the Selective Reenlistment Bonus is in place for high-end operators and senior enlisted members who agree to a four-year obligation. The Marine Corps established a new military occupational specialty and directed targeted incentives to retain cyber talent. The Navy uses the Selective Reenlistment Bonus to retain the most critical enlisted skill sets. The Air Force instituted retention bonuses for enlisted cyber operators and cyberspace operations officers, and also drastically changed its assignments process by implementing back-to-back cyber operational tours. More detail about what each Service is using to incentivize and retain its military workforce is included below:

(U//~~FOUO~~) **Army** – Expanded compensation for cyber Soldiers via Assignment Incentive Pay up-to $500/month for difficult-to-fill Cyber Mission Force (CMF) work roles budgeting $1.6 million annually for 1,850 eligible positions. Special Duty Assignment Pay up-to $300/month in place for 1,245 eligible enlisted cyber positions with an annual budget of $108K. Selective Reenlistment Bonus (SRB) up-to $72k for high-end operators and up-to $100k for senior NCOs agreeing to a four-year obligation. Warrant Officers retention and strength/recruitment remains a challenge with branch transfers, retention bonus, and incentive pay in the works at HQ Department of the Army G1. The Army is also exploring a "tool developer" career field that would keep an officer cohort in a progression path that values keyboard-heavy "hands-on" assignments rather than the more traditional leadership path.

(U) **Marine Corps (USMC)** – Established a new military occupational specialty and directed targeted incentives to maximize the bonus structure to get after and retain special cyber/Information technology (IT) talent. Additionally, 1k growth in FY18 USMC end strength significantly contributed to cyber readiness, doubling the size of Marine Corps Forces Cyberspace Command. Ongoing initiatives in the USMC include building the cyber schoolhouse to train its new cyber Military Occupational Specialty. The USMC is discussing the notion of a "platoon of warrant officers" – this harkens to the reality that as officer's fleet up to leadership positions they often leave technical, hands-on positions. A warrant officer career track could keep "hackers" and "tool developers" deeply technical with their hands always on the keyboard.

(U) **Navy** – Meeting retention goals for cyber-skilled officer and enlisted and using the Selective Reenlistment Bonus (SRB) to successfully retain the most critical enlisted skill sets. Recent NAVADMIN increased award levels and program scope, specifically targeting cyber/intel rates with $30-90K award ceilings. Closely monitoring effectiveness of SRB as civilian job market improves and cyber demand increases. The Navy is also reviewing additional incentives for critical skill sets such as Interactive On-Net Operators (IONs).

(U) **Air Force** – Airmen in Cyberspace Operations Officer career field w/in 4-12 years of service are offered $60k bonus for an additional four-year active-duty service obligation (ADSO). Retention bonus instituted for enlisted cyber operators includes $300/month incentive. Instituting back-to-back CMF tours for CMF-trained personnel ensuring a return on investment and assisting with retention. The Air Force is exploring how to "sharpen and hone" the cyber "reps and sets" of its Airmen. Also tied closely to the mission is "freedom of action" which speaks to the authorities necessary to consistently exercise "reps and sets" in the cyber domain.

(U) **Coast Guard** – The Coast Guard is examining retention incentives, such as Critical Skills Retention Bonus (CSRB), for fully qualified cyber professionals. Coast Guard anticipates offering enlisted members, who are eligible to reenlist in FY19, a $50,000 CSRB for an additional four years of obligated service. Coast Guard employees with federally insured student loans in Cybersecurity job series may also be offered student loan repayment as a recruitment and retention incentive. Coast Guard personnel assigned to Coast Guard Cyber Command are eligible to receive Special Duty Assignment Pay (SDAP). Enlisted members assigned to CGCYBER, who have a final clearance, have completed formal training, and have earned the requisite competencies and qualifications for their watch station receive $75/month.

(U) **AREAS FOR CONGRESSIONAL SUPPORT**

(U) **Tax Code**

(U) On 1 January 2018 the "Tax Cut and Jobs Act of 2017" took effect, changing the entitlements that are considered taxable during a permanent change of station move for civilians. This change disproportionately affects overseas moves. USCYBERCOM relies heavily on civilians to complete the build of its Cyber Operations Integrated Planning Elements within other Combatant Commands. This new law poses significant risk to the ability of the Command to fill these positions. Congress can assist by reassessing the sections in this legislation that apply to civilians and extend the same exemption that exists for uniformed services members of permanent change of station taxes.

(U) **CONCLUSION**

(U) Whether civilian or military, the men and women of U.S. Cyber Command are committed to being part of something bigger than themselves. USCYBERCOM recognizes there is competition for cyber talent; however, our team also realizes working for DOD transcends financial incentives, which speaks to the sense of ethos, patriotism and the opportunity to serve the Nation. USCYBERCOM's unique mission is a key incentive to attracting and retaining cyber talent. Nowhere else can people call themselves cyber warriors who maintain cyberspace superiority through continuous, full-spectrum cyberspace operations that build resilience at home and further our Nation's national security objectives while also contesting those of our adversaries.