

(U) INTRODUCTION

(U) Good afternoon. We have continued Defensive operations to proactively defend the Nation and the DODIN from 2+3 threats as well as the posturing of forces for rapid response.

I intend to highlight:

- Election Defense of the 2020 General Elections
- Hunt Forward Operations
- Defensive Cyberspace Operations against (b)(1)
- Operations to Defend the DoD's Information Network (DoDIN),
- Cyber Mission Force readiness.

(NO Placemat #) (U) ELECTION DEFENSE

- (U) Our guidance from the Secretary is that defending elections is an enduring mission of the Department of Defense.
- (U) We are supporting a whole-of-government effort to defend the 2020 elections.
- (U) The department, through U.S. Cyber Command and the National Security Agency's combined Election Security Group is complementing other Federal Departments through use of our unique authorities and proactive strategic approach to defend forward.
 1. FY19 NDAA (Section 1642) - Counter active, systemic, and ongoing campaigns in cyberspace by our adversaries against the Government and people of the United States
 2. FY19 NDAA (Section 1632) - Clarification that certain cyber operations and activities are traditional military activities.
- (U) We are countering interference and covert foreign influence against our elections by:
 1. (b)(1)
 2. (U) Enabling domestic partner agencies by sharing indications and warnings of indicators of compromise or threat activity with DHS to better protect our systems or providing the FBI information to expose covert influence online.
- (U) Domestically, our collaboration and unity of effort work with DHS has

Copy #:	21-F-0310
Case #:	22-5E-015
SCI #:	
Document #:	2
OSD/JS - FOID	
SCI CONTROL STAMP	
(17)	

~~CONFIDENTIAL - DISSEM ONLY~~

included:

- Established Executive Steering Group to coordinate DoD-DHS collaboration for the protection of critical infrastructure from cyber threats.
- Combined public-private training events with DHS and private sector entities to enable DoD cyber forces to understand domestic critical infrastructure they may be called upon to defend.
- Collaboration to exchange threat information with private sector entities to enable our understanding of adversary cyber TTPs
- Exercised with DHS to refine our respective roles and procedures during a cyber incident; and
- Conducted combined planning to, if DHS requested, ensure DoD would be prepared to augment DHS' cyber incident response elements.
- Finalizing MoA between DHS and DoD to implement Section 1650 of the FY19 NDAA which authorizes DoD to provide DHS up to 50 cybersecurity technical personnel on a non-reimbursable basis to enhance cybersecurity cooperation, collaboration, and unity of government efforts.

(b)(1)



(b)(1)



(U) Q: In what countries have you conducted Hunt Forward Operations?

(b)(1)



(U) Katie Sutton -Q: Will we be able to receive the Hunt Forward Nomination Packages? Similarly, may we receive an After Action Report (AAR) for an operation that's completed? We understand Congress will not receive nomination packages prior to an operation, but we are asking for Congress to receive a copy of a nomination package for an operation that has already concluded.

- (U) A: We can offer to provide briefing to discuss the planning, the execution, and the post-execution activities and outcomes for a completed Hunt Forward Operation.

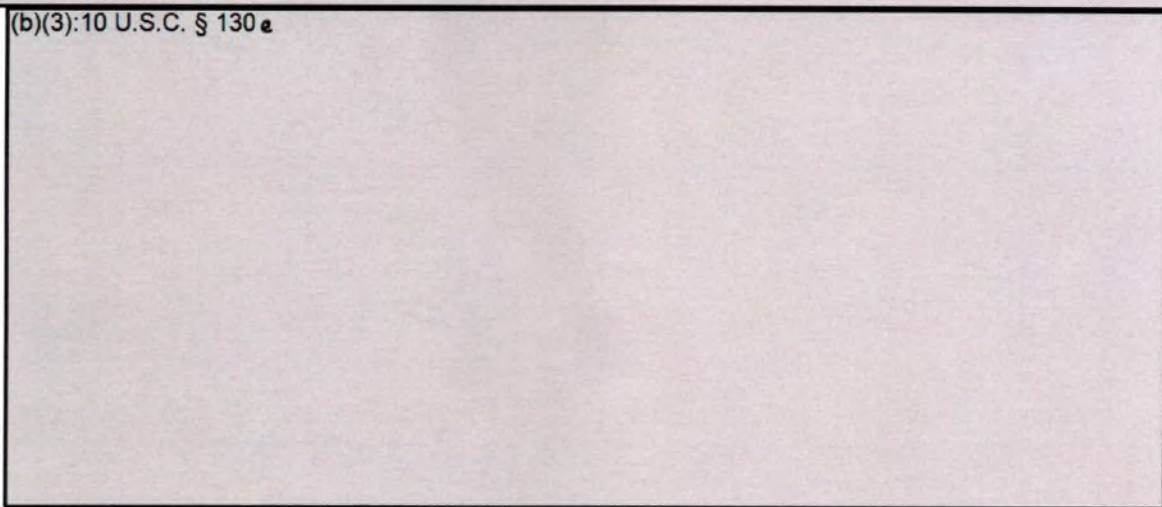
(b)(1)



(b)(1)



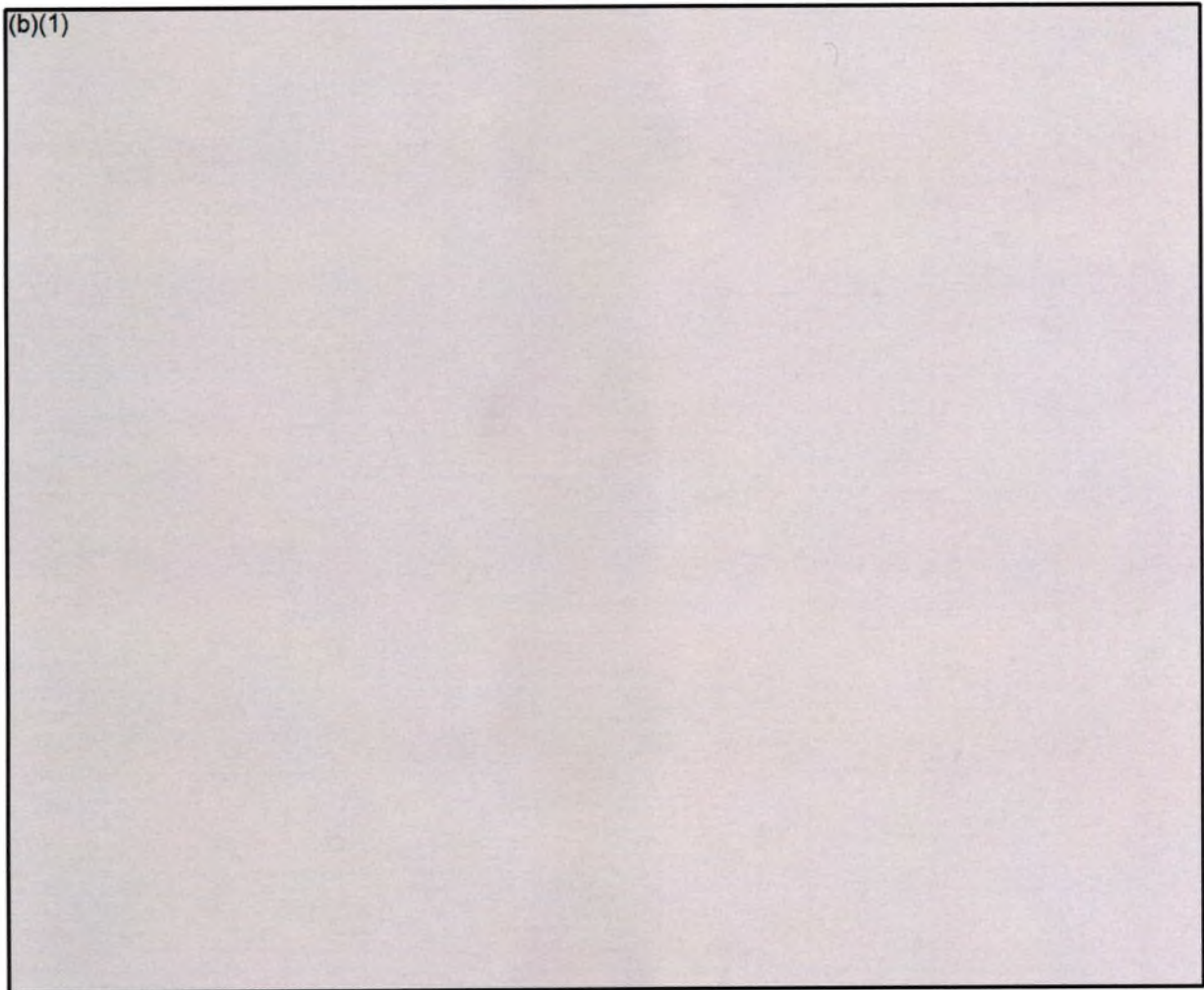
(b)(3):10 U.S.C. § 130 *a*



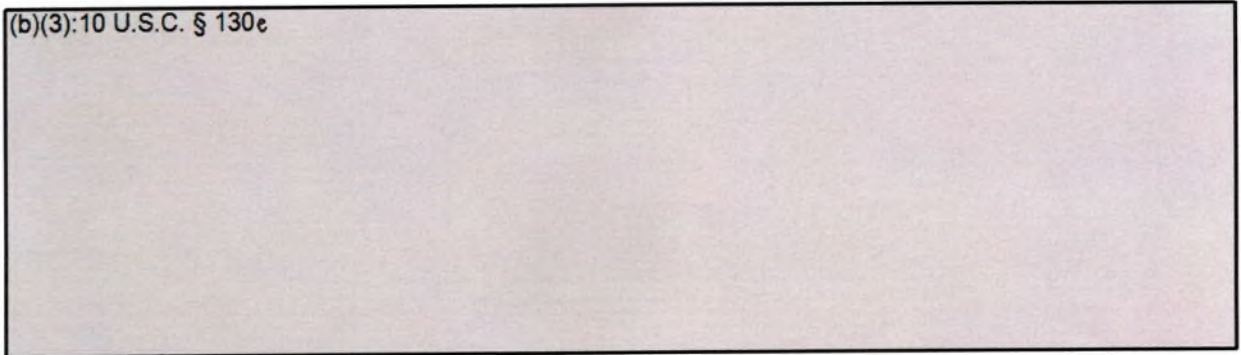
(b)(1)



(b)(1)



(b)(3):10 U.S.C. § 130e



(U) Way Ahead.

- (b)(1)
- (b)(3):10 U.S.C. § 130e

~~(U//FOUO)~~ GLOBAL CAMPAIGN OPERATIONS

~~(U//FOUO)~~ **GLADIATOR SHIELD Campaign**

As I previously briefed, GLADIATOR SHIELD is an overarching campaign which nests within the National and Defense Cyber Security Strategies. It's five major Lines of Operations are **Organize, Secure, Operate, Defend, and Partner**.

(b)(1)



(b)(1)

(Moving to Placemat #BLUE 5) (U//~~FOUO~~) Again under Organize the DoDIN,

(b)(3):10 U.S.C. § 130e

(b)(3):10 U.S.C. § 130e

(Moving to Placemat# BLUE 6)

(b)(1)

(b)(1)

(b)(3):10 U.S.C. § 130 e

(b)(1)

(Moving to Placemat# BLUE 7)

(U//~~FOUO~~) Under Operate the DODIN, (b)(3):10 U.S.C. § 130 e

(b)(3):10 U.S.C. § 130 e

- (U//~~FOUO~~) Forward facing websites which have not met the security requirements are disconnected from the DoDIN

(b)(1)

(NO Placemat #) Cyber Mission Team and Cyber Support Team Readiness

(b)(1)

(b)(1)

Readiness of Cyber Mission Forces.

We acknowledge that the FY2020 NDAA amends Sec. 484 of title 10 USC to add an overview of Cyber Mission Force (CMF) readiness to recurring quarterly cyber operations briefings to the Congressional Defense Committees NLT 180 days after NDAA enactment (20 JUN 2020).

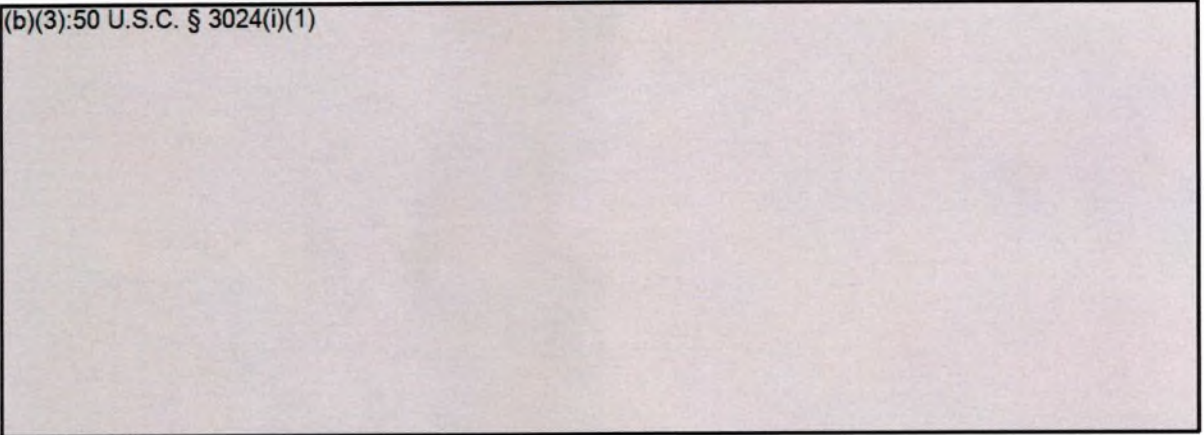
- committed to providing Congress with increased awareness and understanding regarding the readiness of Cyber Mission Forces
- we will ensure DoD reports Cyber Mission Force readiness and reporting as part of the regular routine force readiness reports and briefings to Congress
- Based on recently enacted changes to Section 482 of title 10, United States Codes is amended to require DoD to report on the second and fourth quarter of each calendar year.
- With your concurrence use our limited time in this forum to focus on elements of Cyber Mission Force Readiness, to the extent to which it directly impacts DoD's ability to execute cyber space operations.

Q: Why is the National Mission Force so small if that's the CMF's primary mission?

(b)(1)

(b)(3):50 U.S.C. § 3024(i)(1)

(b)(3):50 U.S.C. § 3024(i)(1)



(b)(1)



(U) CONCLUSION

(U) Our relationships with federal, state, local, industry and international

~~TOP SECRET SI KNOCK~~

partners is critical to everything the Department is doing in the cyber domain. We appreciate your continued support in providing the authorities that allow us to strengthen these partnerships and achieve our national objectives in cyberspace to protect and defend the nation. I look forward to your questions. Thank you.

Election Security Talking Points

(b)(1)

(U//~~FOUO~~) DoD's efforts in preparations for this election cycle are underpinned by the Election Security Group (ESG), a joint USCYBERCOM-NSA Task Force under the command of General Paul Nakasone, the Commander of USCYBERCOM and Director of the National Security Agency.

(b)(1)

- (U//~~FOUO~~) The "Cyber 9-Line" report is a 24/7 communication path between National Guard units and USCYBERCOM; partnerships between state and federal defensive cyber units allows almost immediate information sharing requisite to repel attacks and follow up by pursuing and attributing malicious actors.

(b)(1)

(U//~~FOUO~~) Adversary Assessment.

(b)(1)

(b)(3):50 U.S.C. § 3024(i)(1)

(b)(1)



~~TOP SECRET//REL TO USA, FVEY~~
~~TOP SECRET//REL TO USA, FVEY~~

~~TOP SECRET//REL TO USA, FVEY~~

~~TOP SECRET//REL TO USA, FVEY~~

