SECRETARY OF DEFENSE
1000 DEFENSE PENTAGON
WASHINGTON, DC 20301-1000

JUL 20 2020

MEMORANDUM FOR ALL DOD PERSONNEL

SUBJECT: Reinforcing Operations Security and the Importance of Preventing Unauthorized Disclosures

Proper Operations Security (OPSEC) is critical to protecting our forces, ensuring our mission success, and implementing the National Defense Strategy. History is full of examples of poor OPSEC leading to the unnecessary loss of life and mission failure, and it can mean the difference between our winning and losing as we face great power competitors that will not hesitate to exploit and weaponize information.

The Department of Defense (DoD) remains committed to transparency to promote accountability and public trust. However, it is important to emphasize that unclassified information is not publicly releasable until it is approved for release by an appropriate authorizing official. Unfortunately, poor OPSEC practices within DoD in the past have resulted in the unauthorized disclosure or "leaks" of controlled unclassified information (CUI), including information to be safeguarded under the CUI category for OPSEC, as well as classified national security information (together referred to here as "non-public information").

Unauthorized disclosures jeopardize our DoD personnel, operations, strategies, and policies to the benefit of our adversaries. Unauthorized disclosures also distract from mission priorities by redirecting the attention and resources of military commanders. Whether poor OPSEC takes the form of careless cyber hygiene, "loose talk" among colleagues, or the willful release of non-public information, the result is the same: unnecessary and increased risk of harm to our fellow Americans and our mission.

Any transmission or communication of non-public information to the public or an unauthorized recipient is considered an unauthorized disclosure. Unauthorized disclosures, regardless of purpose or intent, can result in adverse personnel action, including unsatisfactory performance evaluations, records of formal counseling, the loss of security clearances or termination of employment, or even criminal prosecutions.

Ongoing reviews reveal a culture of insufficient OPSEC practices and habits within the DoD. My goal, through an OPSEC campaign, is to change that culture across DoD by reminding DoD personnel to:

1. Be deliberate and careful with all classified, controlled unclassified, and pre-decisional policy information and proposals. Just because someone has a clearance, or previously worked for DoD, does not mean they have a need to know. You must protect non-public information appropriately when communicating with any party, including ensuring that the person receiving the information is authorized access and has a need-to-know or lawful government purpose for such information prior to any disclosure.

2. Comply with DoD policies regarding public disclosures. Ensure that an appropriate DoD Public Affairs office authorizes the release of official DoD information to the news

media, or that information is released according to appropriate procedures (e.g., Freedom of Information Act).

3. Comply with all prepublication review policies, with which you are required to comply even after you retire, resign, or are dismissed from your Government service or contract.

4. Comply with security clearance-related obligations to report certain contacts to your security offices.

5. Review current DoD-wide and organization-specific OPSEC and traditional security practices, and ensure compliance with those procedures.

As part of this OPSEC campaign, I am directing all unit commanders and DoD Component heads to conduct a training period during which all personnel will take training courses on OPSEC and other security policies. Within the next 60 days, all DoD personnel, including civilians, service members, and on-site contractors, are directed to take the Center for the Development of Security Excellence OPSEC Awareness, Unauthorized Disclosure of Classified Information for DoD and Industry, Insider Threat Awareness, and Introduction to Information Security courses (all available at https://securityawareness.usalearning.gov/2020-dod-security-stand-down) or authorized DoD Component equivalents.

I have directed the Under Secretary of Defense for Intelligence Security to take several actions to assess and improve our OPSEC and other security-related postures, policies, requirements, practices, and, importantly, accountability.

The provisions in this memorandum are consistent with and do not supersede, conflict with, or otherwise alter DoD employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this memorandum and are controlling.

Sound OPSEC practices are critical to enhancing the Nation's safety, prosperity, and competitiveness. I am confident that all DoD personnel, whether service members, civilians, or contractors, understand the importance of OPSEC to the safety of our warfighters and the success of our important national security missions. Now is the time to reinvigorate our focus on OPSEC to improve our security practices, and remain vigilant with ourselves and our colleagues. OPSEC must be everyone's responsibility.