DEPARTMENT OF THE AIR FORCE
WASHINGTON DC 20330-1000

APR 1 8 2023

Airmen and Guardians,

Last week, the Federal Bureau of Investigation arrested an Airman for an alleged significant classified breach with potential impact on the conflict in Ukraine and our relationships with our allies and partners. Given the seriousness of this situation, the Department of the Air Force is closely examining all security measures and protocols to ensure we do all we can to protect sensitive information.

Securing classified national security information is a crucial aspect of the profession of arms. Last week, the Deputy Secretary of Defense sent a memorandum reiterating our responsibilities regarding safeguarding classified information. On 17 April, Secretary Austin released the attached plan for an immediate review and assessment of the Department's information security procedures; this memorandum reinforces that guidance.

Executive Order 13526 states the unauthorized disclosure of Secret information could be expected to cause serious damage to national security and the unauthorized disclosure of Top Secret information could be expected to cause exceptionally grave damage to national security. Safeguarding national security information is not limited to ensuring personnel possess the appropriate clearance and training, they must also have the need to know. All of us are responsible for obeying and enforcing the rules that protect classified information.

Safeguarding national security information is a commander's responsibility. All leaders are responsible for ensuring personnel are properly trained, security procedures are followed, and need-to-know determinations are deliberate. Upon receipt of this memorandum all commanders will initiate an immediate review to assess their adherence to the standards set forth in Secretary Austin's guidance. More information will follow this memorandum with specific tasks.

In addition, we will be directing a security focused standdown be conducted in the next 30 days at each unit. The focus of the standdown will be to reassess our security posture and procedures, validate the need to know for each person's access, and emphasize to all Airmen and Guardians the responsibility we are entrusted with to safeguard this information and to enforce and improve our security requirements.

We must be continually alert for personnel who should not have access or who do not possess the need-to-know for specific classified information. Enforcing the need-to-know requirement is a chain of command responsibility -- these are important, conscious choices leaders must make at every level to guarantee our Nation protects the crucial information required to negotiate the complex and competitive strategic environment we are in today.

As Secretary Austin recently stated, "the recent unauthorized disclosures are a stark reminder security procedures in both the cyber and physical domain are foundational to the Department's mission success." "As leaders, we rely on commanders, supervisors, and security managers at all levels of the chain of command to lead by example, to hold their personnel appropriately accountable, and to continuously reinforce the obligations of those we have entrusted with the Nation's secrets to protect classified national security information."

We know you understand the seriousness of the profession you all have volunteered for and we trust you to uphold the highest standards of conduct at work and at home. Thank you for continuing to serve in the world's greatest Air Force and Space Force.

One Team, One Fight!

Frank Kendall
Secretary of the Air Force

Charles Q. Brown, Jr.
General, U.S. Air Force
Chief of Staff

B. Chance Saltzman
General, U.S. Space Force
Chief of Space Operations

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

APR 17 2023

MEMORANDUM FOR ALL DEPARTMENT OF DEFENSE PERSONNEL

SUBJECT: Immediate Review and Assessment of Department of Defense Information Security Procedures

Reference: (a) DoDM 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," incorporating Change 2, July 28, 2020.
(b) DoDM 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information" incorporating change 2, July 28, 2020.
(c) DoDI 5230.09, "Clearance of DoD Information for Public Release" incorporating change 1, February 9, 2022.
(d) DoDI 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019.
(e) "Review of Department of Defense Security Policies and Procedures," Secretary of Defense Memorandum, April 14, 2023.

Adverse security incidents are a stark reminder that adherence to required security procedures underpin all aspects of the Department of Defense (DoD) mission, and we must continually reinforce these requirements to keep pace with evolving threats. It is therefore essential to carefully examine the sufficiency of, and compliance with, all security policies and procedures.

As leaders, we rely on commanders, supervisors, and security managers at all levels of the chain of command to lead by example, to hold their personnel appropriately accountable, and to continuously reinforce the obligations of those we have entrusted with the Nation's secrets to protect classified national security information (CNSI). Leaders at all levels must immediately reiterate to their workforce the vital importance of strict adherence to security procedures for access to, protection of, and proper handling of CNSI.

On April 14, 2023, I directed the Under Secretary of Defense for Intelligence and Security (USD(I&S)), in coordination with the DoD Chief Information Officer (CIO) and the Director of Administration and Management (DA&M), to lead a comprehensive 45-day review of DoD security programs, policies, and procedures in reference (e). In the interim, DoD Components will immediately review and assess their adherence to the following standards for protecting CNSI, and report their findings to the USD(I&S), no later than May 2, 2023.

As outlined in Enclosure 3 of reference (a) and Enclosures 2 through 5 of reference (b), DoD Components must ensure their organizations adhere to the following standards:

- **Accountability**: DoD Components are required to comply with policy requirements to designate a TOP SECRET (TS) Control Officer and maintain a system of

accountability to record the receipt, reproduction, transfer, transmission, downgrading, declassification, and destruction of TS information.

- **Safeguarding:** DoD Components are required to re-emphasize control measures, to re-emphasize compliance with pre-publication review processes specified in reference (c); to validate the security clearance and "need to know" for individuals requesting CNSI; and to ensure end of day security checks are conducted. Additionally, all DoD Components that are not an Intelligence Community element are required to conduct a 100% review and validation of the continuing need for their assigned personnel to be indoctrinated into Sensitive Compartmented Information.

- **Storage and Destruction:** Classified information is required to be secured and maintained under conditions adequate to deter and detect access by unauthorized persons. This includes General Services Administration-approved containers, Director of National Intelligence-approved requirements for Sensitive Compartmented Information, and locks approved by the DoD Lock Program (information available here: https://locks.navfac.navy.mil). To promote "clean desk" environments, personnel must appropriately destroy non-record copies of CNSI when those documents are no longer necessary for ongoing tasks.

- **Transmission and Transportation:** Components are required to ensure CNSI is appropriately packaged in transit, using lock bags or other approved means, and transported by credentialed couriers. Furthermore, at all times DoD personnel are required to follow transportation policy and procedures between accredited secure spaces.

- **Security Education and Training:** DoD Components are required to ensure compliance with security and education policy which includes mandatory initial and annual refresher training for CNSI and Controlled Unclassified Information, which exceeds the Federal government standard for such training every other year.

- **Reporting of Security Incidents Involving Classified Information:** All DoD personnel who become aware of the loss or potential compromise of CNSI are required to immediately report such information to their chain of command and their security manager. DoD personnel may also report incidents to their Office of the Inspector General.

- **Cybersecurity Protocols:** For the purposes of electronic transmission, DoD personnel are required to transmit CNSI only over secure communications networks approved for the transmission of information at the specified level of classification. DoD Components are required to immediately review their adherence to existing policies and guidance to ensure compliance with system access controls, auditability, and user activity monitoring on classified networks. Components should further adhere to the principle of "least privilege" access to classified data.

- **Transmission on Private Sector Communications Channels Expressly Prohibited:** In accordance with reference (d), non-DoD-controlled electronic messaging services are not authorized to process non-public DoD information, regardless of the service's perceived appearance of security (e.g., "private" social media accounts or groups, "protected" or "encrypted" messaging applications, such as WhatsApp, Signal, etc.).

Leaders must reinforce their expectation that their workforce will immediately report all security incidents to the chain of command and their security manager or the Office of their Inspector General, and must ensure individuals in their workforce are empowered to make these reports. In addition, DoD Components should leverage their supporting counterintelligence and security professionals to provide refresher training to the workforce. This training should address the risks and consequences of unauthorized disclosures, which may include, administrative penalties, such as termination of employment, or criminal prosecution, as appropriate.

DA&M will promulgate initial actions to implement this guidance for the Office of the Secretary of Defense. The DoD CIO will also immediately issue additional guidance for the Department. These actions and measures may include, but will not be limited to: restriction or deletion of distribution lists on classified computer networks, allowing limited physical and electronic access to certain intelligence products, granting printing privileges on the Joint Worldwide Intelligence Communications System by exception, requiring proper information handling procedures including encryption of emails, and increasing inspections when people enter and exit Sensitive Compartmented Information Facilities.

Based on these finding and the broader 45-day review cited in reference (e), the Under Secretary of Defense for Intelligence and Security, in coordination with the DoD CIO and DA&M, will advise me on any necessary security policy changes, including those related to the aforementioned standards and will identify forward any enhanced requirements for those with access to our most sensitive systems, information, and facilities.