INFORMATION SECURITY OVERSIGHT OFFICE
NATIONAL ARCHIVES *and* RECORDS ADMINISTRATION
700 PENNSYLVANIA AVENUE, NW, ROOM 100 WASHINGTON, DC 20408-0001
www.archives.gov/isoo

September 7, 2018

MEMORANDUM FOR THE SENIOR AGENCY OFFICIAL FOR THE CONTROLLED UNCLASSIFIED INFORMATION (CUI) PROGRAM AT THE U.S. DEPARTMENT OF HOMELAND SECURITY (DHS)

SUBJECT: Provisional Approval of CUI Categories

In response to your letter dated December 4, 2017, I want to first apologize for the delay in providing a reply. I provisionally approve all of the information types referenced in your letter and authorize their inclusion in the CUI Registry under the following conditions. This approval letter in and of itself is not an authority pursuant to law, regulation, or government-wide policy for safeguarding and dissemination controls. DHS must:

- Sponsor, issue, or coordinate a suitable law, Federal regulation, or Government-wide policy (authority) for all or each of the provisionally approved categories;
- Coordinate with the CUI Executive Agent any authority that the agency proposes to use for all or each of the provisionally approved categories; and
- Provide quarterly updates on your agency's progress in sponsoring, issuing, or coordinating a suitable authority.

Note: Updates must be provided to cui@nara.gov.

Protection of Provisional Categories

Provisional categories of CUI shall be:

- **Marked** as CUI using the CUI Control Marking (i.e., CUI) in accordance with marking guidance found on the CUI Registry;
- **Protected** in accordance with 32 CFR Part 2002, "Controlled Unclassified Information" and for *Homeland Security Agreement Information* and for *International Agreement Information*, in accordance with any existing information sharing agreements; and
- **Disseminated** in accordance with any limited dissemination control markings applied to the information. The CUI Registry lists all limited dissemination control markings that can be applied to CUI.

Establishment Provisional Categories

The following information types are approved as provisional categories of CUI. When there is overlap with existing CUI Categories, and if applicable, the requirements from existing categories must be followed.

1. **Homeland Security Agreement Information** is defined as information DHS receives and is required to protect pursuant to an agreement with state, local, tribal, territorial, and private sector partners. DHS receives this information in furtherance of the missions of the Department, including but not limited to, support of the Fusion Center Initiative and activities for cyber information sharing consistent with the Cybersecurity Information Security Act.

2. **Homeland Security Enforcement Information** is defined as unclassified information of a sensitive nature lawfully created, possessed, or transmitted by DHS in furtherance of its immigration, customs, and other civil and criminal enforcement missions, the unauthorized disclosure of which could adversely impact the mission of the Department.

3. **International Agreement Information** is defined as information DHS receives and is required to protect pursuant to an information sharing agreement or arrangement with a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.

4. **Information Systems Vulnerability Information (ISVI)** means:

   a. DHS information technology internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need. Examples of information are systems inventories and enterprise architecture models. Information pertaining to national security systems and eligible for classification under Executive Order 13526, will be classified as appropriate.

   b. Information regarding developing or current technology, the release of which could hinder the objectives of DHS, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to close, counterfeit, or circumvent a process or system.

5. **Operations Security Information** is defined as unclassified information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten/compromise operations security.

6. **Personnel Security Information** is defined as information that could result in physical risk to DHS personnel or other individuals that DHS is responsible for protecting.

7. **Physical Security Information** is defined as assessments or reports illustrating or disclosing facility infrastructure or security vulnerabilities related to the protection of federal buildings, grounds, or property, such as threat assessments, system security plans, contingency plans, risk management plans, business impact analysis studies, and certification and accreditation documentation.

8. **Privacy Information** includes information referred to as Personally Identifiable Information (PII). PII embodies information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

9. **Sensitive Personally identifiable Information (SPII)** is a subset of PII that, if lost, compromised or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Some forms of PII are sensitive as stand-alone elements.

a. Examples of stand-alone PII include: Social Security Numbers (SSN), driver's license or state identification number; Alien Registration Numbers; financial account number; and biometric identifiers such as fingerprint, voiceprint, or iris scan.
b. Additional examples of SPII include any groupings of information that contain an individual's name or other unique identifier plus one or more of the following elements:

   i. Truncated SSN (such as last four digits)
   ii. Date of birth (month, day, and year)
   iii. Citizenship or immigration status
   iv. Ethnic or religious affiliation
   v. Sexual orientation
   vi. Criminal history
   vii. Medical information
   viii. System authentication information such as mother's maiden name, account passwords, or personal identification numbers

c. Other PII may be "sensitive" depending on its context, such in as a list of employees and their performance rating(s) or an unlisted home address or phone number. In contrast, a business card or public telephone directory of agency employees contains PII, but is not sensitive.

Questions regarding these provisionally approved categories can be directed to the DHS CUI Program Manager, Scott Ackiss, scott.ackiss@hq.dhs.gov.

Mark A. Bradley

MARK A. BRADLEY
Director