SLIDE 1: [OPENING (AOTUS)]

The National Archives and Records Administration plays a critical role in American statecraft by protecting, and managing the exchange of information resources between Executive Branch agencies and their non-federal partners.

An essential component of The National Archive's responsibility as the Executive Agent in marshalling this flow of information is the Controlled Unclassified Information – or CUI – program, administered through the Information Security Oversight Office.

We appreciate the sharing and protecting of information under the CUI Program as an art practiced by civil servants in every department and agency, and their non-federal partners, working on behalf of the American people.

Practicing this art sets into motion the creative potential of government operations under the law, and requires the mastery of basic concepts and tools standardized across the government, but implemented through the policies and procedures of every federal agency.

In support of the interagency CUI program, the discussions that follow explain these concepts and tools, so fundamental to the entire lifecycle of Controlled Unclassified Information:

The definition of CUI, and the distinctions between types of information provided in the CUI Registry;

The principles of access and sharing as they apply to Lawful Government Purpose and limited dissemination control markings;

Marking requirements overall,
for email, and for packages and standard mail;

Controlled Environments, both physical and electronic;

The Reproduction of CUI;

FAXing CUI;

Reporting incidents;

The Destruction of CUI; and

The acceptable indicators for the Decontrol of CUI.

SLIDE 2: What is CUI?

CUI, Controlled Unclassified Information, is sensitive information that requires protection under laws, regulations and Government-wide policies – protection that Executive Branch agencies have been doing for decades, but on an ad hoc and inconsistent basis.

In the slides that follow we will discuss the types of information protected under the CUI program.

SLIDE 3: Lawful Government Purpose

Lawful Government Purpose is the standard for granting access to CUI. Access to CUI should be granted to individuals performing

"any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes [as] within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement)."

As a dynamic standard this concept focuses on the purposes CUI may serve as a resource in achieving the mission objectives of government operations and projects. Although not required, in principle CUI **should be** shared when the contents of CUI will help achieve the goals of a common project or operation. If sharing CUI would obstruct or harm the government purpose, do not share the CUI.

SLIDE 4: The CUI Registry

The CUI Registry, available online, is the catalogue of information types under the CUI Program. These information types include, for example: Privacy, Tax, Critical Infrastructure, Law Enforcement, Proprietary, Intelligence, Legal, and Financial information.

Executive Branch Agencies use the CUI Registry to implement the CUI Program through their own policies and procedures.

For practitioners, the CUI Registry provides training modules on topics from Marking to Destruction, and other resources such the Marking Handbook, CUI Coversheets, and links to access the CUI blog where you can find additional guidance.

SLIDE 5: CUI Basic and CUI Specified

Before Marking CUI, it is important to understand that there are two types of CUI:

CUI Specified is sensitive information for which laws, regulations and Government-wide polices – or authorities - call for specific protections.

For CUI Basic the authorities do not.

CUI Specified must be marked in a different way.

SLIDE 6: Marking

Marking is the first step in the proper handling of CUI.
Marked CUI informs the user or recipient of the information's status.
A banner heading must appear at the top of each page of documents containing CUI.
Banners may contain up to three elements – with each element separated by two forward slashes:

1) Control Marking – The Control Marking must always appear in the banner as either the word "CONTROLLED" or "CUI" at the top of the page. For CUI Basic, the Control Marking is all that is required.
2) The Category Marking is only required for CUI Specified categories. The Category Markings found on the CUI Registry must follow two forward slashes after the Control Marking, and preceded by "SP-" [S P DASH].
3) Agencies my also apply optional Limited Dissemination Control Markings, as found on the CUI Registry, according to Agency policies and procedures.

SLIDE 7: Marking Email

Marking CUI in Email follows the same principles for marking CUI in other contexts:
Banner Markings must appear above the email text containing CUI;
As a best practice, the Subject Line may also indicate the email contains CUI.
File Names for any attachments containing CUI, may also include an indicator that alerts the recipient to the presence of CUI.
Be sure to include all applicable markings when forwarding or responding to emails that contain CUI.

SLIDE 8: How to Send CUI in Packages and Mail

When shipping CUI, you may use interagency mail systems, the United Postal Service, or any commercial delivery service.
As a best practice, use in-transit automated tracking to record the progress of your shipment from departure to arrival.
And remember: the contents of packages must be appropriately marked, but do not place markings on the outside of packages or envelops.

SLIDE 9: Controlled Environments: Physical

CUI must be stored or handled in controlled environments that prevent or detect unauthorized access.

A Controlled Environment is any area or space with adequate physical or procedural controls to protect CUI from unauthorized access or disclosure.

In physical environments, physical barriers must prevent or detect unauthorized access to CUI. Should unauthorized access occur, the physical barrier in place should show evidence of tampering.

When not under the direct control of an Authorized Holder, CUI must be protected with at least one physical barrier that protects against unauthorized access. Barriers should show evidence of tampering or alteration.

Examples of physical barriers include: sealed envelopes, locked doors, overhead bins, drawers, or file cabinets. Agencies may employ key control procedures or electronic access devices to limit or control access to areas where CUI is stored, handled, or processed.

Common areas or public areas, such as cafeterias, waiting areas, or public transportation systems, are not acceptable for the storage, discussion, or review of CUI.

Be aware of your surroundings and ensure that CUI is adequately protected.

SLIDE 10: Controlled Environments: Electronic

In the electronic environment, barriers should exist that limit access to only those with a Lawful Government Purpose. Barriers include:

Dedicated network drives, file folders, or **intranet** sites

Electronic environments must also prevent or protect CUI from unauthorized access.

Notably, under these requirements, existing safeguards that meet the standards for handling classified information are sufficient for protecting CUI.

Organizations should establish procedures to ensure that only authorized individuals have access to CUI. These procedures should also remove access when it is no longer required.

In short, Controlled Environments, whether physical or electronic, facilitate access to CUI by Authorized Users with a lawful government purpose, by safeguarding CUI from access by Unauthorized Users.

SLIDE 11: Reproducing CUI

When Reproducing or FAXing CUI, you may use agency-approved equipment. Agencies may put signs on approved equipment.

SLIDE 12: Reporting CUI Incidents

Incidents involving CUI must be immediately reported. Agencies and organizations must have means - such as hotlines, email address, or points of contact - for employees to report incidents.

SLIDE 13: What to Report

CUI incidents include but are not limited to:

- Improper storage of CUI
- Actual or suspected mishandling of CUI
- When unauthorized individuals gain access to CUI (physical or electronic)
- Unauthorized release of CUI (to public facing websites or to unauthorized individuals)
- Suspicious behavior from the workforce (Insider Threats)
  - General disregard for security procedures
  - Seeking access to information outside the scope of current responsibilities
  - Attempting to enter or access to sensitive areas (where CUI is stored, discussed, or processed)

Know what to report, and follow your agency policy and procedures regarding how to report incidents

SLIDE 14: Destroying CUI

CUI must be destroyed to a degree that makes the information unreadable, indecipherable, and irrecoverable. This means that in paper form, you should not be able to make out a letter or a number once the information is destroyed. On this slide you see an example of shred participles that do not meet the standard for destroying CUI.

SLIDE 15: Signs for Approved Destruction Equipment and Methods

Destruction equipment or methods should be identified with signs or placards alerting you to what equipment or methods are approved for destruction.

Some organizations use “destruction bins” to destroy their CUI. These bins should have signs on them indicating that it is acceptable to deposit CUI within them. These bins should also be locked to prevent any unauthorized access.

NEVER use a standard trash can or recycling bin when throwing out CUI!

SLIDE 16: Decontrol and Marking

CUI may be decontrolled when it no longer requires protection in accordance with an underlying authority, or agency policy.

Decontrolled CUI must have a marker or indicator on the first page to indicate that the information is no longer CUI. Agency policy will provide additional guidance on the methods and procedures for decontrolling CUI at your agency.

Agency policies may require handlers to strike through, or to remove old CUI markings either on the first page, cover page, or the first page of any attachment.

Decontrolled CUI is still subject to the release procedures of your agency.

SLIDE 17: Additional Resources

For more information on the CUI Program and its elements, please visit the CUI Registry. From the CUI Registry you will find training videos, and additional resources to increase your understanding of these concepts.

SLIDE 18: [Closing: AOTUS]

Today, the art of sharing and protecting CUI grows ever more critical
to defending the foundations of our American Republic, and to achieving the potentials of government operations under the democratic institutions
launched by our Revolutionary founders.

I appreciate the mastery of fundamental CUI concepts and tools
across the federal government, and by our partners outside of government,
as I look forward to the continuing success of the interagency CUI program.

Thank you.