OFFICE of
information
technology
services

GUIDE TO DATA & SYSTEMS CLASSIFICATION

Data is a valuable and vulnerable asset of the state. This document establishes guidance to keep data secure and mitigate associated risks of data breaches, hacks, and cyberattacks.

Table of Contents

Introduction

Purpose

This guide outlines the Idaho Technology Authority's (ITA) data classification framework to ensure proper handling, labeling, and protection of information based on its sensitivity and potential impact if breached. It supports compliance with P4130 – Information Systems Classification Policy - Idaho Technology Authority and federal Controlled Unclassified Information (CUI) requirements.

When to Use

When classifying data or/and systems.

What is data classification?

Data classification involves categorizing and labeling information to:

- Protect sensitive data based on its security requirements.
- Mitigate risks of breaches or unauthorized disclosures.
- Enhance data management, compliance, and decision-making.
- Reduce storage and backup costs through efficient tracking.

What is system classification?

System classification is the process of categorizing systems based on their sensitivity, criticality, and impact.

- **Risk-Based Categorization**: Systems are classified according to their potential risks, including threats to confidentiality, integrity, and availability.
- **Compliance & Regulatory Alignment**: Classification helps ensure adherence to security frameworks like NIST 800-53, and industry-specific regulations.
- **Access & Protection Levels**: Higher-classified systems require stronger security controls, limiting access and enforcing encryption, auditing, and monitoring.
- **Operational Impact & Dependency**: Classification accounts for the system's role in business operations, ensuring resilience and incident response measures match its criticality.

Scope

All state employees and systems on the state network.

Classification Levels

ITS Classification Framework

The framework defines four (Unrestricted, Limited, Restricted, Critical) classification levels based on sensitivity, value, and impact, aligned with FIPS-199 standards. FIPS 199, Standards for Security Categorization of Federal Information and Information Systems | CSRC

Classification Level 1: "Unrestricted": Commonly referred to as public data, includes information relating to the conduct or administration of a state agency and is typically created specifically for public consumption. Examples: public websites, brochures, and public employee contact information.

Classification Level 2: "Limited": Commonly referred to as internal data, includes sensitive information that may or may not be protected from public disclosure. Examples: audit reports, email and other communications, and building schematics.

Classification Level 3: "Restricted": Commonly referred to as confidential data, includes sensitive information intended for agency use only and is typically federally regulated. Examples: network diagrams, protected health information (PHI), and personal identifiable information (PII).

Classification Level 4: "Critical": Highly sensitive information where disclosure could cause significant harm, including potential injury or death. Examples: Investigative reports of criminal activity, record of undercover police officers, etc.

Table 1: Data Classification Examples

Data Classification			
Level 1 | Unrestricted | Public	Level 2 | Limited | Internal	Level 3 | Restricted | Federal	Level 4 | Critical
- Press releases - Brochures - Public websites - Published research - Materials created for public consumption	- Internal audit reports - Financial transactions - Emails - Non-public phone numbers - Building schematics - Names and addresses that are not protected from disclosure	- Employee records - Financial data - Internal reports - Personal contact details - Social Security Number (SSN) - Driver's license number - Passport number - Tax returns - Fingerprint data - Warrants or restraining orders - Medical records - Credit card numbers (PAN)	- Disclosure that could result in loss of life, disability, or serious injury - Regulated information with significant penalties for unauthorized disclosure. This information is typically exempt from public disclosure

Table 2: System Classification Examples

Data Classification			
Level 1 | Unrestricted | Public	Level 2 | Limited | Internal	Level 3 | Restricted | Federal	Level 4 | Critical
Systems that handle Level 1 data	Systems that handle Level 2 data	Systems that handle Level 3 data	Systems that handle Level 4 data

Key Considerations

- **Aggregation Impact:** Combining data elements (e.g., PII like name and SSN) may elevate the classification to the highest level of any single element.
- **System Classification:** Systems storing mixed data are classified at the highest level of data they contain.

Personally Identifiable Information (PII)

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of information. When several elements of PII are combined, this can increase the potential harm if disclosed without authorization. Idaho Code Title 28, Chapter 51 defines "personal information" as an Idaho resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted:

- Social security number
- Driver's license number or Idaho identification card number
- Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account.

The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.

PII Confidentiality Impact Factors

Several factors contribute to determining the impact from a loss of confidentiality of PII. Factors provided below should be considered in conjunction. One factor by itself may indicate a low impact level, but another factor might indicate a high impact level, in turn overriding the first indication of low impact.

1. **Identifiability**: Does the data directly identify an individual (e.g., SSN vs. ZIP code)?
2. **Quantity**: What is the total number of individuals whose data is involved?
3. **Data Field Sensitivity**: Does combining data increase risk (e.g., name + financial details)?
4. **Context**: Does the use case affect sensitivity (e.g., public newsletter vs. undercover officer list)?
5. **Legal Obligations**: Are there laws mandating protection (e.g., HIPAA)?
6. **Access/Location**: Is data accessed frequently or stored offsite?

Data Labeling and Handling

All data must be labeled to reflect its classification, using Microsoft Purview for documents, emails, and presentations. If a system or volume contains multiple classifications, label it with the strictest level. The reference tables below provide examples of classification labeling and data handling.

Microsoft Purview for CUI

There are limitations to what can be accomplished for marking CUI therefore users will need to ensure proper markings even if the automated solution fails to accurately mark the item. Refer to the CUI section of this document for further information.

Table 3: Classification Labeling Examples

Media	Classification Level 1 | Unrestricted | Public	Level 2 | Limited | Internal	Level 3 | Restricted | Federal	Level 4 | Critical
Electronic Media Email/Text Recorded Media CS/DVD/USB (Soft Copy)	External **and** Internal labels Email – Beginning of subject line Physical Enclosure - Label	Creation Date Applicable Statute, if known (i.e. Idaho Technology Authority P4130) External **and** Internal labels Email – Beginning of subject line Physical Enclosure - Label	Creation Date Applicable Statute, if known (i.e. Idaho Technology Authority P4130) External **and** Internal labels Email – Beginning of subject line Physical Enclosure – Label (Reference IRS Pub 1075 for additional marking requirements for FTI)	Applicable Statute (i.e. Idaho Technology Authority P4130) (i.e., Federal requirements per E.O. 13526) Non-shareable Will remain in approved systems only Accessed only by approved users
Hard Copy	Each page if loose sheets; Front **and** back covers **and** title page if bound	Each page if loose sheets; Front **and** back covers **and** title page if bound	Each page if loose sheets; Front **and** back covers **and** title page if bound	Hard-copy production is not authorized
Web Sites	**Public Facing Website** Each page labeled "Public" on bottom of page	**Internal Website Only** Each page labeled "LIMITED" on top **and** bottom of page	**Internal Website Only** Each page labeled "HIGHLY RESTRICTED" on top **and** bottom of page	**Not Authorized for Any Website** Each system page labeled "CRITICAL" on top **and** bottom of page Page WARNING required

Table 4: Data Handling Requirements

Method of Transfer or Communication	Classification Level 1 | Unrestricted | Public	Level 2 | Limited | Private	Level 3 | Restricted | Confidential | Federal	Level 4 | Critical
Non-Disclosure Agreement (NDA)	No NDA requirements	No NDA requirements	NDA is recommended prior to access by non-ITS employees.	NDA is required prior to access by non-ITS employees.
Internal Network Transmission (wired & wireless)	No special requirements	No special requirements	- Encryption is required - Instant messages are prohibited - FTP is prohibited	- Encryption is required - Instant messages are prohibited - FTP is prohibited
External Network Transmission (wired & wireless)	No special requirements	- Encryption is recommended - Instant message with caution - FTP is prohibited	- Encryption is required - Instant messages are prohibited - FTP is prohibited - Remote access should be used only when necessary and only with VPN and MFA	- Encryption is required - Instant messages are prohibited - FTP is prohibited - Remote access is prohibited
Copying	No restrictions	Permission of data custodian advised	Permission of data custodian required	Permission of data custodian required
Data at Rest (file servers, databases, archives, etc.)	- Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Encryption is recommended - Logical access controls are required to limit unauthorized use - Physical access restricted to specific groups	- Encryption is required - Logical access controls are required to limit unauthorized use - Physical access restricted to specific individuals	- Encryption is required - Logical access controls are required to limit unauthorized use - Physical access restricted to specific individuals
Mobile Devices (cell phone, tablets, etc.)	No special requirements	- Encryption is recommended - Remote wipe should be enabled, if possible	- Encryption is required - Remote wipe must be enabled, if possible	- Encryption is required - Remote wipe must be enabled, if possible
Email (with and without attachments)	No special requirements	- Encryption is recommended	- Encryption is required - Do not forward	- Encryption is required - Do not forward

Physical Mail	No special requirements	- Mail with agency interoffice mail - US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	- Mark "*Open by Addressee Only*" - Use "*Certified Mail*" and sealed, tamper-resistant envelopes for external mailings - Delivery confirmation is required - Hand delivering is recommended over interoffice mail	- Mark "*Open by Addressee Only*" - Use "*Certified Mail*" and sealed, tamper-resistant envelopes for external mailings - Delivery confirmation is required - Hand deliver internally
Printer	No special requirements	- Verify destination printer - Retrieve printed material without delay	- Verify destination printer - Use secure print - Attend printer while printing	- Verify destination printer - Use secure print - Attend printer while printing
Web Sites	No special requirements	Posting to publicly accessible Internet sites is prohibited	Posting to publicly accessible Internet sites is prohibited	Posting to publicly accessible Internet sites is prohibited
Telephone	No special requirements	Confirm participants on the call line	- Confirm participants on the call line - Ensure private location	- Confirm participants on the call line - Ensure private location
Video / Web Conference Call	No special requirements	- Roster of attendees - Confirm participants on the call line	- Pre-approve roster of attendees - Confirm participants on the call line - Ensure private location	- Pre-approve roster of attendees - Confirm participants on the call line - Ensure private location
Spoken Word	No special requirements	Reasonable precautions to prevent unintentional disclosure	Active measure to control and limit information disclosure to authorized individuals	Active measure to control and limit information disclosure to authorized individuals
Fax	No special requirements	- Verify destination number - Confirm receipt	Faxing is prohibited	Faxing is prohibited

Controlled Unclassified Information (CUI)

CUI is unclassified federal information requiring protection under E.O. 13556, Executive Order 13556 – Controlled Unclassified Information | whitehouse.gov. Idaho agencies handling Level 2 (Limited) or Level 3 (Restricted) data shared with federal agencies must comply with CUI requirements per NIST SP 800-171r3, SP 800-171 Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations | CSRC.
National Archives and Records Administration (NARA) is the Executive Agent (EA) that maintains the CUI registry and associated website, Controlled Unclassified Information (CUI) | National Archives.
State of Idaho employees: the-handling of CUI must be in accordance with E.O. 13556, 32 CFR Part 2002, eCFR :: 32 CFR Part 2002 -- Controlled Unclassified Information (CUI), supplemental guidance published by the CUI Executive Agent and all applicable EA-approved agency policy. This publication provides guidance on what each marking is, where and how to apply it, and which items are mandatory or optional.
Since CUI is a federal information handling requirement it is more likely that a federal entity will own the CUI labeling requirements and share the already labeled CUI with an Idaho state entity. In such instances the Idaho agency will not be required to mark the information but must adhere to handling requirements of the CUI material.

NIST SP 800-171r3 CUI Overlay

The NIST SP 800-171r3 CUI Overlay is a control overlay spreadsheet, available on csrc.nist.gov, that contains the CUI requirements which are based on the NIST SP 800-53r5 controls and NIST SP 800-53B moderate control baseline. The CUI Overlay is useful for comparing required CUI controls with those found within an agencies specific Information Security Policy.

The CUI Registry

The CUI Registry serves as the government-wide central repository for all information, guidance, policy, and requirements on handling CUI. It includes authorized CUI categories, associated markings, handling and decontrolling procedures. National Archives and Records Administration (NARA) is the Executive Agent (EA) that maintains the CUI registry and associated website, Controlled Unclassified Information (CUI) | National Archives.

CUI Types

- **CUI Basic**. Standard controls apply (e.g., general sensitive data).
- **CUI Specified**. Specific handling controls mandated by law (e.g., Protected Critical Infrastructure Information).

Table 5: Types of CUI

CUI Basic	CUI Specified
Sensitive information with no additional or different requirements mentioned in the underlying authorities. CUI Basic does not provide specific guidance and a majority of CUI will be CUI Basic.	*Sensitive information whose underlying authority has specified something different or extra is required for that type of information (i.e. limited distribution, additional protections, etc.). CUI Specified is not a higher level of CUI.*
Authorized users need to understand which authority applies to their specific information. The authority listed in the CUI Registry Category List, Controlled Unclassified Information (CUI) | National Archives, will state if the information is CUI Basic or CUI Specified.	

CUI Safeguarding

Authorized holders of CUI are responsible for complying with applicable safeguarding requirements in accordance with 32 CFR 2002, this guidance, and all applicable guidance published in the CUI Registry.
All CUI authorized holders of CUI Specified materials must follow the applicable procedures in the underlying laws, regulations, or government-wide policies for the CUI Specified materials. Only categories designated in the CUI Registry, may be implemented for designating materials.
Authorized holders of CUI must verify the recipient(s) of CUI have an appropriate need for access to the CUI in furtherance of a lawful government purpose and must ensure the recipient(s) continue upholding the CUI requirements.

- **Training:** Authorized holders must complete CUI training.
- **Labeling:** Use CUI banner markings (e.g., "CUI//SP-PCII//NOCON") per the CUI Registry.
- **Processing:** Do not process CUI on personally owned electronic devices unless connected through an approved agency system with approved controls in place.
- **Storage:** Store in encrypted, FISMA-moderate systems, not personal devices.
- **Transmission:** Encrypt emails with CUI attachments; use secure file shares (e.g., DoD SAFE).
- **Destruction:** Shred to 1mm x 5mm particles or sanitize per NIST SP 800-88.

Marking CUI

Authorized holders of CUI must verify the recipient(s) of CUI have an appropriate need for access to the CUI in furtherance of a lawful government purpose and must ensure the recipient(s) continue upholding the CUI requirements.

Websites.

Websites containing CUI will have restricted access, password protection, MFA and indicate the presence of CUI with a splash screen WARNING. See below.

Graphic 1: Website WARNING

WARNING

This is an ITS State of Idaho computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Use of this system indicates consent to monitoring and recording. Individuals found performing unauthorized activities may be subject to disciplinary action including criminal prosecution. This system contains Controlled Unclassified Information (CUI). All individuals viewing, reproducing or disposing of this information are required to protect it in accordance with 32 CFR Part 2002.

CUI Banner Marking

The CUI banner marking appears at the top of each page of any document that contains CUI and is mandatory for all documents containing CUI. The content of the banner marking must be inclusive of all CUI within the document and must be the same on each page. The banner marking should appear as bold, capitalized black text and be centered when feasible. The banner marking may include up to three elements:

- Control Marking: example "CUI", mandatory for all CUI
- Category or subcategory: example "SP-PCII/SAFE", alphabetized; mandatory for CUI Specified.
- Dissemination Control: example "NOCON", optional; indicates restrictions (e.g., no contractors).

Table 6: CUI Banner Marking Segments

CUI Control Marking	CUI Category or Subcategory Marking	Limited Dissemination Control Marking
CUI//	CATEGORY/SUBCATEGORY	//DISSEM

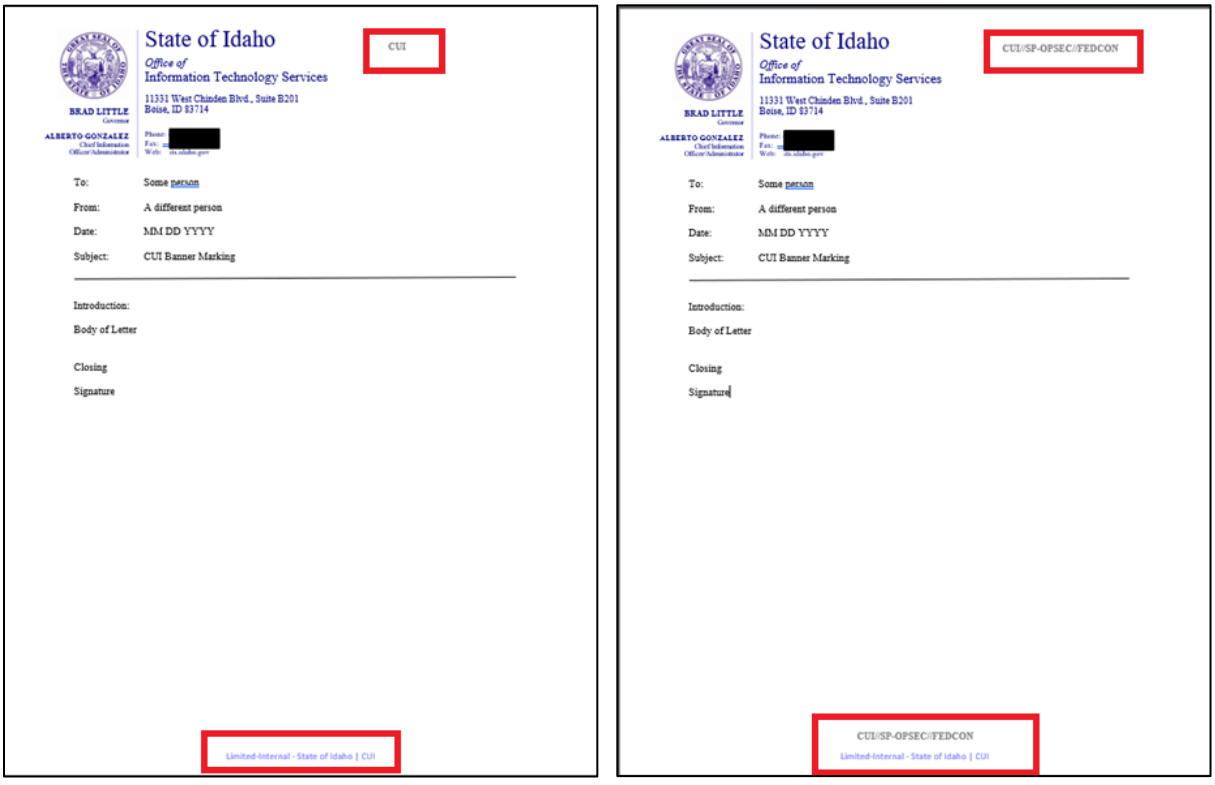
Note: the above example uses the words “CATEGORY”, “SUBCATEGORY”, and “DISSEM” as substitutes for the actual markings found in the CUI Registry. Consult the CUI Registry for actual markings.

Documents

As an optional best practice, the CUI Banner Marking may be placed at the bottom of the document as well. Below are two examples showing the options for the CUI Banner Marking.

Graphic 2: Memo Banners & Markings

Mandatory: CUI Banner Markings must appear on the top portion of the page. Due to the agency memo standard marking, the Purview auto label will be hidden behind and the author must manually enter the CUI banner in the header. The example memo on the left shows a CUI Basic Banner Marking while the example memo on the right shows a CUI Specified Banner



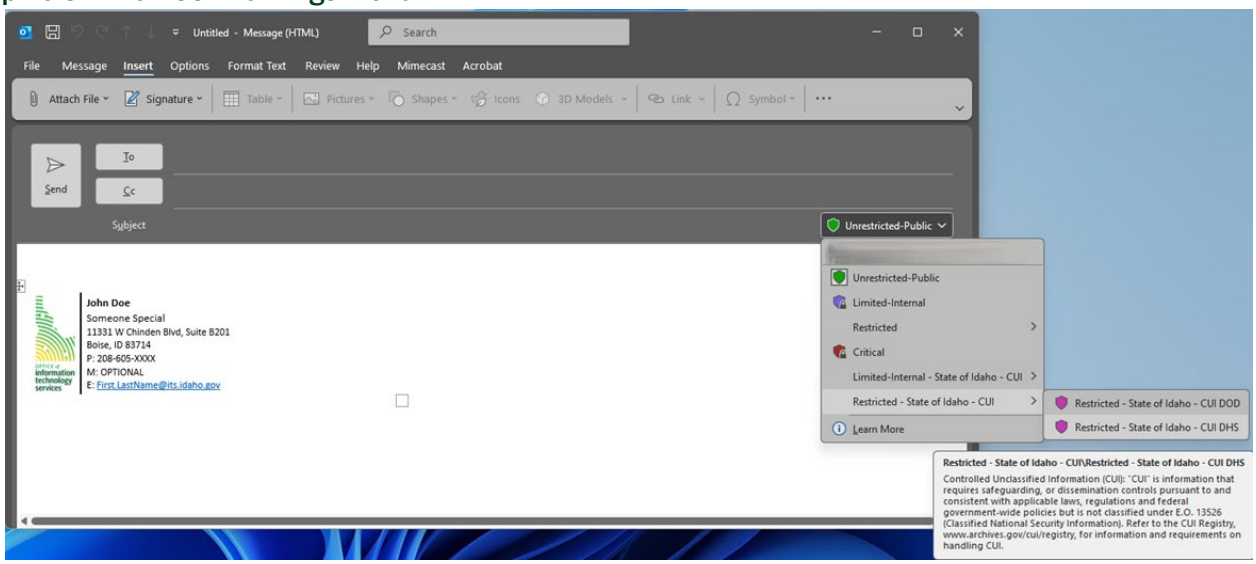
Optional Best Practice: CUI Banner Markings placed bottom center. When using Purview to auto label the memo, the State of Idaho classification will be entered before the CUI Basic Banner Marking (memo on left). Due to limitations of Purview, the CUI Specified Banner Marking will need to be added manually above the Purview auto label.

Emails

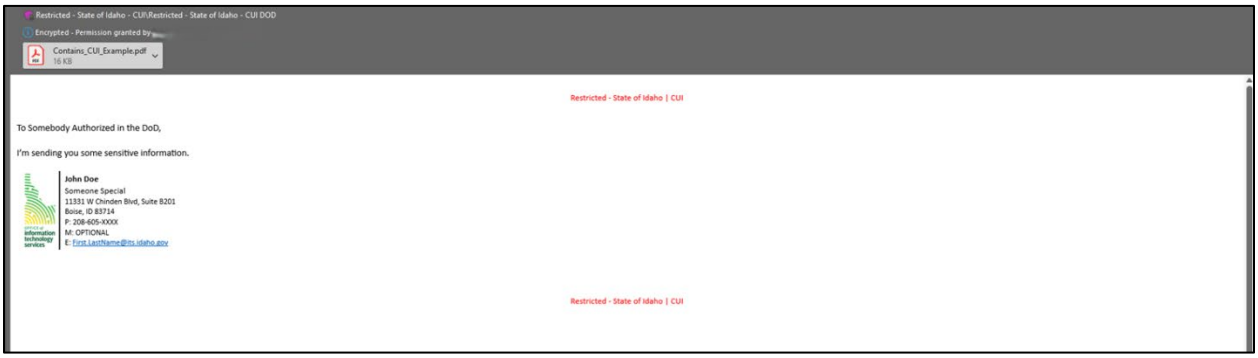
ITS created a menu in Purview, available in Microsoft Outlook, for selecting the data classification level of emails. The first four options are specific to State of Idaho data classification and there are two subcategory options for pairing State of Idaho data classification with CUI data classification. Only State of Idaho – Limited and State of Idaho – Restricted will use CUI data classification. These options will only be used if the state agency is communicating CUI with a federal agency.

The Purview menu option currently offers two subcategories (based on most likely federal agencies to require CUI), under the State of Idaho – Limited and State of Idaho – Restricted categories. The CUI DoD and CUI DHS options provide a statement regarding CUI. The resulting banner marking will meet the intent of CUI marking, however only for CUI Basic. If CUI Specified markings are required, the author of the email is required to add the specified markings in addition to selecting the menu option labeling. Currently Purview in Outlook will not allow the author of the email to visualize the applied header and footer. Only the recipient of the email will see the header and footer applied.

Graphic 3: Email CUI Markings Menu



Graphic 4: Email CUI Markings – Received email

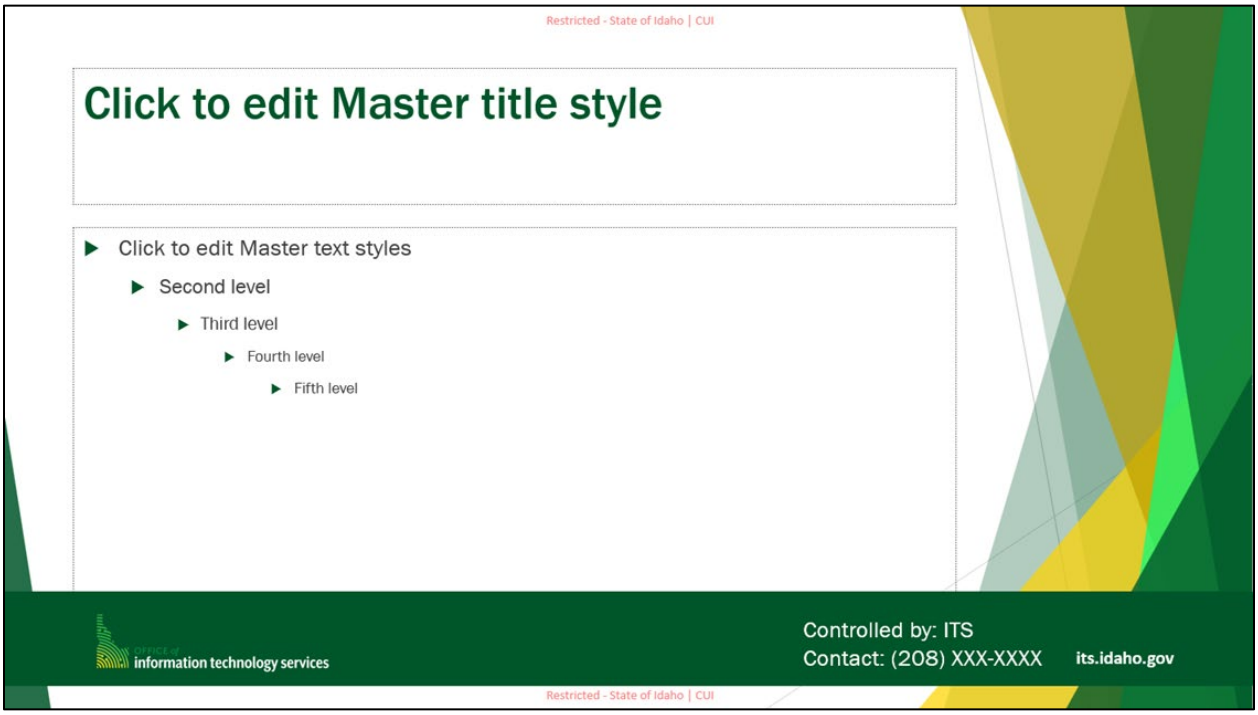


CUI Markings for Slide Presentations

Below is an example of applying CUI Banner Markings to a PowerPoint presentation. The presentation creator will need to select from the Purview menu for the specific label required. As shown in the graphic

below, the header and footer are automatically applied to the slide. Current limitations with Purview prevent the addition of CUI Specified markings. If CUI Specified markings are required, the presentation creator is responsible for their addition. The addition of the designation indicator is required due to presentation slides not typically being created with agency contact information as would be found in a memo address block or email signature block.

Graphic 5: Slide Presentation Markings



Designation Indicators for CUI

Designation indicators are pieces of information that indicate the designator's agency and are required for any use of CUI. Designators may be the use of letterheads, a signature block with agency, or the use of a 'controlled by' line. A specific point of contact, an office or division should include contact information for anyone that has questions concerning the CUI.

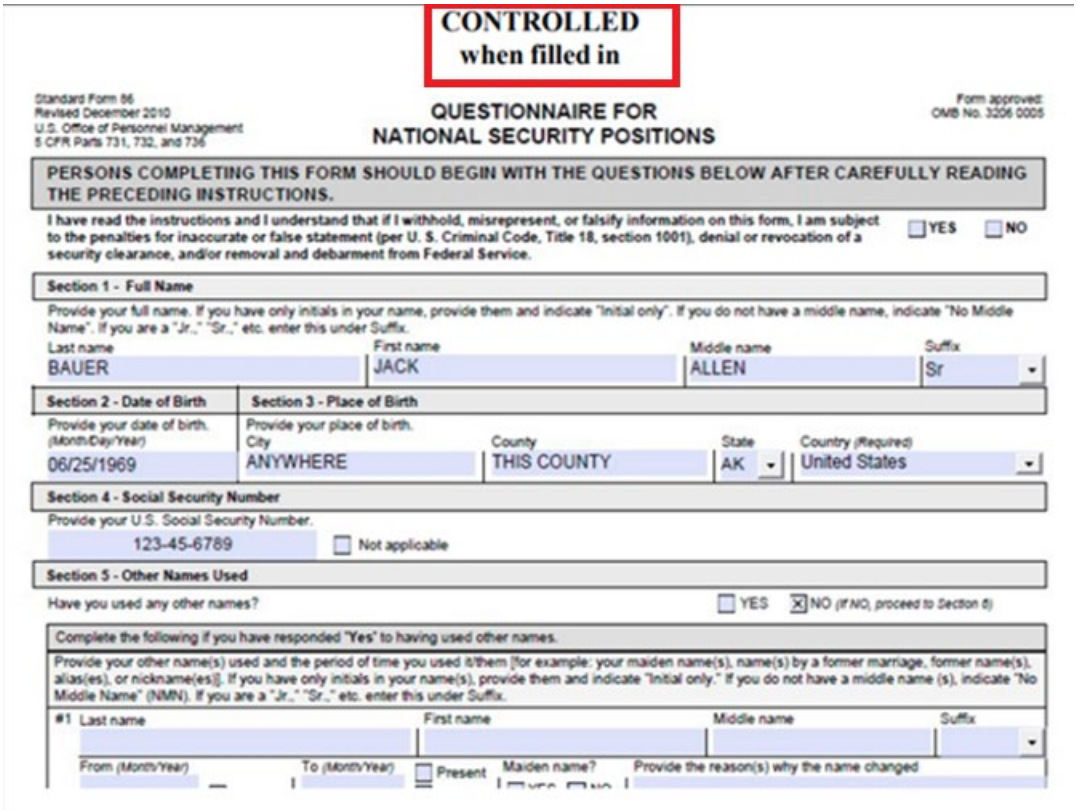
CUI Marking - Electronic Media Storing or Processing

Media such as thumb drives, hard drives, CD ROMs, DVDs, etc. must be marked to alert holders to the presence of CUI stored on the device. It may not be possible to include CUI Category, Subcategory, or Limited Dissemination Control Markings due to space limitations (i.e. thumb drives) but at a minimum the CUI Control Marking and the designating agency must be displayed.

CUI Markings for Forms

Forms that contain CUI must be marked accordingly when filled in. If space is limited, then a coversheet should be used. As the forms are updated agencies will comply with the CUI Program and include a statement that indicates the form is CUI when filled in.

Graphic 6: Form, CUI when filled in



CONTROLLED
when filled in

Standard Form 86
Revised December 2010
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

QUESTIONNAIRE FOR
NATIONAL SECURITY POSITIONS

Form approved:
OMB No. 3206 0005

PERSONS COMPLETING THIS FORM SHOULD BEGIN WITH THE QUESTIONS BELOW AFTER CAREFULLY READING THE PRECEDING INSTRUCTIONS.

I have read the instructions and I understand that if I withhold, misrepresent, or falsify information on this form, I am subject to the penalties for inaccurate or false statement (per U. S. Criminal Code, Title 18, section 1001), denial or revocation of a security clearance, and/or removal and debarment from Federal Service. ☐ YES ☐ NO

Section 1 - Full Name

Provide your full name. If you have only initials in your name, provide them and indicate "Initial only". If you do not have a middle name, indicate "No Middle Name". If you are a "Jr.," "Sr.," etc. enter this under Suffix.

Last name	First name	Middle name	Suffix
BAUER	JACK	ALLEN	Sr

Section 2 - Date of Birth

Provide your date of birth. (Month/Day/Year)
06/25/1969

Section 3 - Place of Birth

Provide your place of birth.

City	County	State	Country (Required)
ANYWHERE	THIS COUNTY	AK	United States

Section 4 - Social Security Number

Provide your U.S. Social Security Number.
123-45-6789 ☐ Not applicable

Section 5 - Other Names Used

Have you used any other names? ☐ YES ☒ NO *(If NO, proceed to Section 6)*

Complete the following if you have responded "Yes" to having used other names.

Provide your other name(s) used and the period of time you used it/them [for example: your maiden name(s), name(s) by a former marriage, former name(s), alias(es), or nickname(es)]. If you have only initials in your name(s), provide them and indicate "Initial only." If you do not have a middle name (s), indicate "No Middle Name" (NMN). If you are a "Jr.," "Sr.," etc. enter this under Suffix.

#1 Last name	First name	Middle name	Suffix

From (Month/Year)	To (Month/Year)	☐ Present	Maiden name?	Provide the reason(s) why the name changed
			☐ YES ☐ NO	

Document Cover Sheet

State of Idaho, Level 2 Limited Cover Sheet

Refer to Annex A: State of Idaho, Level 2 Limited Cover Sheet for an example. The header of the cover sheet indicates the State of Idaho data classification level. The background color is purple for Level 2 Limited data classification.

There are two separate texts boxes within the cover sheet. The top box is for list State Handling Procedures, in accordance with law, policy and guidance. Also included in the top box will be the designated information controller, the category of data included, specific dissemination controls, designation indicators, customer name, various information pertaining to the specific communication between the agencies, a warning for the individual handling the information, and handling instructions. The lower text box communicates Federal handling procedures and requirements.

State of Idaho, Level 3 Restricted Cover Sheet

Refer to Annex B: State of Idaho, Level 3 Restricted Cover Sheet for an example. The header of the cover sheet indicates the State of Idaho data classification level. The background color is yellow for Level 3 Restricted data classification.

There are two separate texts boxes within the cover sheet. The top box is for list State Handling Procedures, in accordance with law, policy and guidance. Also included in the top box will be designated the information controller, the category of data included, specific dissemination controls, designation indicators, customer name, various information pertaining to the specific communication between the agencies, a warning for the individual handling the information, and handling instructions. The lower text box communicates Federal handling procedures and requirements.

CUI Cover Sheet

Refer to Annex C: CUI Cover Sheet for an example. The header of the cover sheet indicates the information is CUI. The background color is a standard purple for all federal data marked as CUI.

There are two separate texts boxes within the cover sheet. The top box is for indicating categories of CUI, limited dissemination controls, special instructions, points of contact, and any other information the owner of the CUI information requires. The lower text box communicates federal handling procedures and requirements.

Event Management

Report Level 2- Limited, Level 3 - Restricted, Level 4 – Critical, and CUI events (e.g., unauthorized disclosure, improper storage, misuse) to the ITS Security Operations Center, soc@its.idaho.gov. Such events are not considered “Incidents” per Idaho Statute and thus will not follow the Incident Response Plan.

Media Sanitation/Destruction

Media Sanitation/Destruction for Data Classifications

Before disposal or re-use, media must be sanitized in accordance with ITS policy (MP-06) Media Sanitization. These methods ensure that data is not unintentionally disclosed to unauthorized users.

Level 1, 2, 3, and 4 Sanitation/Destruction

Physical media (printouts and other physical media) must be disposed of by one of the following authorized means which includes thorough burning or shredding:

- When burning the data, the material must be burned in an incinerator that produces enough heat to burn the entire bundle, or the bundle must be separated to ensure that all pages are incinerated.
- When shredding the data, destroy paper using crosscut shredders which produce particles that are 1mm x 5mm (.04in. x .2in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 2.4mm (3/32in.) security screen.

Electronic media (hard drives, tape cartridge, CDs, printer ribbons, flash drives, printer, and copier hard drives, etc.) must be disposed of by one of the following authorized means:

- Overwriting (at least 3 times) - an effective method of clearing data from magnetic media. As the name implies, overwriting uses a program to write (1s, 0s, or a combination of both) onto the location of the media where the file to be sanitized is located.
- Degaussing - a method to magnetically erase data from magnetic media. Two types of degaussing exist: strong magnets and electric degausses. Note that common magnets (e.g., those used to hang a picture on a wall) are weak and cannot effectively degauss magnetic media.
- Destruction – a method of destroying magnetic media. As the name implies, destruction of magnetic media is to physically dismantle by methods of crushing, disassembling, etc., ensuring that the platters have been physically destroyed so that no data can be pulled.

Table 7 Media Sanitation/Destruction for Data Classification Requirements

	Classification			
	Level 1 | Unrestricted | Public	Level 2 | Limited | Private	Level 3 | Restricted | Federal	Level 4 | Critical
Electronic Media Sanitization	Not Required (Recommended)	Mandatory	Mandatory	Mandatory
Physical Media Destruction	Not Required (Recommended)	Mandatory	Mandatory	Mandatory

CUI Sanitation/Destruction

- Destroy per NIST SP 800-88 SP 800-88 Rev. 1, Guidelines for Media Sanitization | CSRC when no longer needed and per agency retention schedules.
- Use locked bins for shredding; contract vendors must protect CUI during disposal.
- Do not destroy CUI at alternate work locations without proper equipment.

Annex A: State of Idaho Limited Cover Sheet

State of Idaho, Level 2 - Limited

ATTENTION: State Handling Procedure

Controlled by: State of Idaho
Classification of data: <Unpublished research, Customer records, Personnel records, non-public policies, non-public contracts, internal memos, unpublished planning, and budgeting info, engineering designs, CUI>
Specific dissemination controls: <Agency specific handling requirements>
If Found Contact #: <Agency contact – First, Last name>; <Agency contact email>

Customer Name: State and Local Governments in Idaho
Project Number:
Internal Part Number:
Date:
Other Data:
Other Data:
Notes or Distribution Statement:

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with ITA P4130 – Information Systems Classification and applicable agency policy.

Access to and dissemination of Idaho data shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

ATTENTION: Federal Handling Procedure

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

State of Idaho, Level 2 - Limited

Annex B: State of Idaho Restricted Cover Sheet

State of Idaho, Level 3 - Restricted

ATTENTION: State Handling Procedure

Controlled by: State of Idaho
Classification of data: <PII, FTI, STI, PCI data Security Standards, SSA, CJI, Information that pertains to the security of data, Information that pertains to the security of facilities, CUI>
Specific dissemination controls: <Agency specific handling requirements>
If Found Contact #: <Agency contact – First, Last name>; <Agency contact email>

Customer Name: State and Local Governments in Idaho
Project Number:
Internal Part Number:
Date:
Other Data:
Other Data:
Notes or Distribution Statement:

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with ITA P4130 – Information Systems Classification and applicable agency policy.

Access to and dissemination of Idaho data shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

ATTENTION: Federal Handling Procedure

All individuals handling this information are required to protect it from unauthorized disclosure.

Handling, storage, reproduction, and disposition of the attached document(s) must be in accordance with 32 CFR Part 2002 and applicable agency policy.

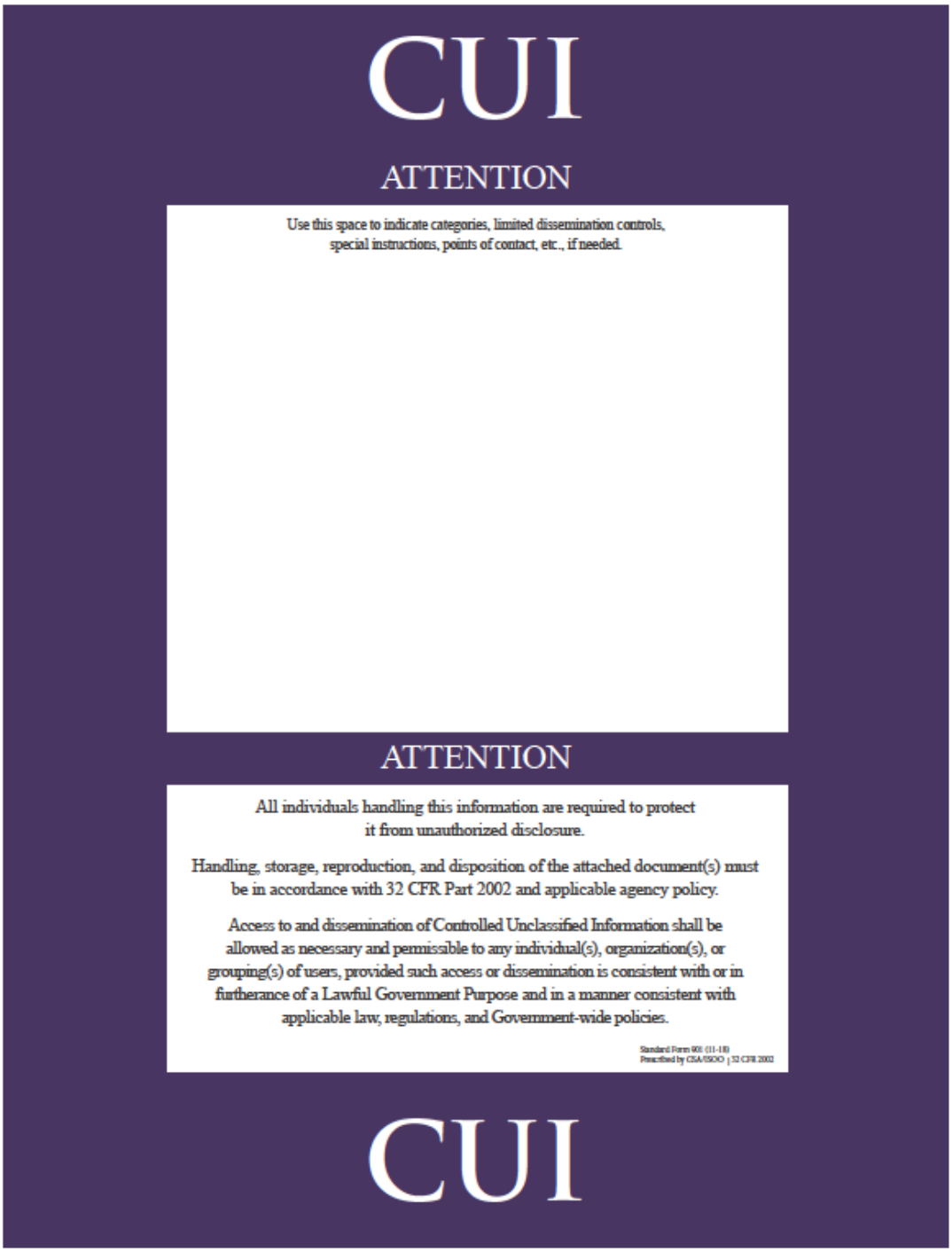
Access to and dissemination of Controlled Unclassified Information shall be allowed as necessary and permissible to any individual(s), organization(s), or grouping(s) of users, provided such access or dissemination is consistent with or in furtherance of a Lawful Government Purpose and in a manner consistent with applicable law, regulations, and Government-wide policies.

Standard Form 901 (11-18)
Prescribed by GSA/ISOO | 32 CFR 2002

State of Idaho, Level 3 - Restricted

Annex C: CUI Cover Sheet

Below is the image of a Standard Form 901 CUI coversheet that can be downloaded from the GSA.gov website. The center light shaded area is where the CUI owner should indicate categories, limited dissemination controls, special instructions, points of contact, etc. if needed.



Annex D: Microsoft Purview Troubleshooting

Initial testing of Purview for data classification labeling revealed several limitations and bugs. There are instances where additional information will need to be added to the header, footer, or both depending on requirements. This section serves to address potential issues encountered.
If adding a custom footer to a document with a sensitivity label causes the label's footer to disappear, it is likely due to a conflict in the document's layout settings, or a problem with the sensitivity label application itself. Most troubleshooting solutions were found using a browser search for the Purview issue observed (i.e. search query – "sensitivity label footer disappears if I add a footer to doc"). Here's a breakdown of potential causes and solutions:

Possible Causes:

- Conflicting Layout Settings: The custom footer might be overriding the sensitivity label's footer, or the document's page margins might be interfering with the label's placement.
- Sensitivity Label Application Issues: There might be a bug or a problem with how the sensitivity label is being applied, preventing it from displaying correctly.
- Version Compatibility: Ensure your version of Office is up-to-date and compatible with the sensitivity label features.
- Section Breaks: If your document uses section breaks, the sensitivity label's footer might only apply to specific sections and not the entire document.

Most Effective Troubleshooting Step:
Initial users found the most effective method for applying a sensitivity label that disappeared, due to additional information being placed into the header or footer, was to select a different (incorrect) sensitivity label. Then, after the incorrect sensitivity label has been applied, reselect the correct sensitivity label, and it appears correctly. This process will generate a justification error box with three options available describing the reason the sensitivity label was changed. Select the appropriate reason and the sensitivity label should be viewable. Double check the labeled item by viewing it in print preview mode.

Additional Troubleshooting Steps:

1. *Check Print Layout View*: Make sure you're in print layout view This view is essential for seeing headers and footers.
2. Verify Sensitivity Label Settings:
    a. Go to "Home" > "Sensitivity" to ensure the correct label is applied.
    b. Check the sensitivity label settings in the Microsoft Purview compliance portal to ensure the label is correctly configured.
    c. Verify that the sensitivity labels are published in the Microsoft Purview compliance portal.
3. Adjust Page Margins:
    a. Go to "Layout" > "Margins" and ensure that the margins are set appropriately to allow enough space for both the custom footer and the sensitivity label's footer.
4. Check Header and Footer Settings:
    a. Double-click in the header or footer area to edit them.
    b. Ensure that the sensitivity label's footer is not being accidentally deleted or hidden.
    c. If you have a custom footer, try removing it temporarily to see if the sensitivity label's footer reappears.
5. *Update Office*: Ensure that your version of Office is up to date to ensure compatibility with the latest sensitivity label features.
6. *Reapply the Sensitivity Label*: Try reapplying the sensitivity label to the document after making any necessary changes to the layout settings.

For additional trouble shooting, query a search browser for the issue observed.