PKH

PKH ENTERPRISES
Where Policy Meets Technology

TITUS

Protect Your CUI Data

5 Steps to Implementing Your CUI Compliance Plan

TITUS White Paper

At TITUS we work to help businesses better manage and secure valuable corporate information. Our focus is on building policy management solutions that make it easier for IT administrators to protect and manage corporate correspondence including email and documents.

For further information, contact us at (613) 820-5111 or email us at info@titus.com

www.titus.com

1.0 | Overview

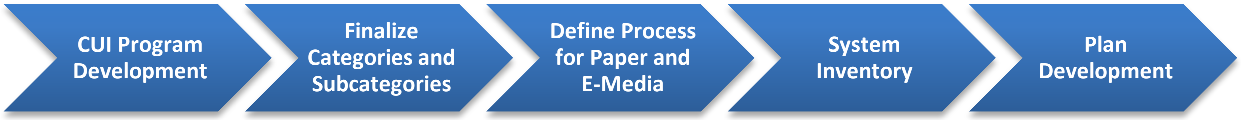
The U.S. Federal Government is currently addressing the challenge of consistency and transparency in handling of Controlled Unclassified Information (CUI). Organizationally, each agency must determine the information that it needs to protect and must develop a compliance plan that defines how they will implement CUI.

With extensive experience helping government agencies protect their sensitive data, PKH Enterprises and TITUS understand both the challenges and the opportunities that are posed by this program. TITUS classification and safeguarding software has been instrumental in helping organizations implement similar programs in Australia and Canada. Agencies have an opportunity to use products, such as those from TITUS, to comply with CUI guidelines and fully leverage their information assets.

2.0 | CUI Framework

Departments and agencies were required to submit a catalogue of proposed CUI categories and subcategories in May 2011. As the next step in CUI implementation, departments and agencies are required to develop an agency compliance plan by December 6, 2011. The CUI Office[1] has just released "CUI Compliance Plans: Overview and Recommendations for Departments and Agencies", which outlines the basic elements in an agency compliance plan.

This white paper describes five steps to develop an agency compliance plan that enables the CUI framework to be an effective mechanism for your agency. The agency compliance plan must lay out your agency's CUI program. This includes the five elements described in the recent CUI office paper: Governance, Policy, Training, Technology, and Self Inspection. The following steps will help to ensure that you have addressed your organization's information needs as you implement CUI:


CUI Program Development
Finalize Categories and Subcategories
Define Process for Paper and E-Media
System Inventory
Plan Development

Step 1 – <u>CUI Program Development</u>: The agency must define who is responsible for CUI management, what resources they have, and how they interact with offices, such as the CIO or Security Office, which are critical to CUI implementation. In developing the CUI program, it is important to understand all of the offices that are impacted by CUI implementation, including organizations that may not be immediately apparent. CUI will impact both information used to accomplish an agency's mission as well as information used administratively (e.g., acquisition, legal and policy).

Given the breadth of CUI, the agency must decide what office has responsibility and authority for CUI implementation. For example, does the office with CUI authority have policy-making authority, and what is the agency's process for promulgating policy? A good goal is to lay out these processes and build relationships in the next two months while building the agency compliance plan. Doing so will bring the internal agency partners into the planning process and ensure the development of an implementable plan. Each agency must establish a CUI program that includes awareness, training, marking guidance, safeguarding and dissemination rules, and acquisition guidance in accordance with the guidelines established by the CUI Office. Please see Appendix 1 for a sample Program Checklist for defining CUI governance, policy/guidance, training, technology and compliance/self-inspection.

[1] Executive Order 13556 designates the National Archives and Records Administration (NARA) as the Executive Agent to implement CUI and oversee agency actions to ensure compliance with this order. The CUI Office fulfills these responsibilities on behalf of NARA.

Step 2 -Finalize Categories and Subcategories: The CUI Office will maintain a CUI Registry that articulates the rules that must be used when handling CUI. Each agency must work with the CUI Office to ensure that the CUI Office understands the agency's information sharing and safeguarding needs so that these needs are reflected in the CUI Registry. It is critical that all the sensitive information that the agency needs in order to accomplish its mission is adequately documented and that sharing and safeguarding rules are articulated properly. It is likely that the coordination of CUI categories across agencies may require changes to agency business procedures. The more that the agency office responsible for CUI integrates with the agency's business needs, the more it can communicate those needs effectively so that any changes do not impact mission capabilities. By coordinating with the CUI Office, an agency can ensure that it is building internal agency policy that supports the federal program and enables the accomplishment of the agency's mission.

Step 3 - Define Process for Paper and E-Media: Information is transferred both by physical and electronic means. Implementation of CUI will require the evaluation of both the means and the potential adjustment of existing processes to comply with the rules and regulations promulgated by the CUI Office. It is important that agencies review the data that they have and the means in which they use that information to accomplish their mission. Movement of paper information can be implemented through defined procedures. In many cases, these procedures are already in place. Electronic transfer may require distinguishing elements of data that fall under each handling rule. It may be the first time that an agency has been required to or implemented this level of differentiation. Tracking the types of data per system and the corresponding data handling rules will require a review of agency data management procedures. In the end, implementing CUI is an opportunity to begin or improve data access by category. As the procedures for both paper and electronic media are defined and refined, agencies can develop appropriate training for the workforce. The following Handling Rules Template will help with this review.

Handling Rules Template

Description of Information	Authority	Safeguarding Rules	Dissemination Rules

Step 4 – System Inventory: In order to effectively implement CUI, agencies must understand what systems in the agency handle CUI information and what categories (and subcategories) of CUI are contained in each system. Doing so allows agencies to evaluate what safeguarding measures are required for each system. Agencies must also consider if the dissemination rules for the CUI categories on a particular system are the same or if there must be access control within the system by CUI category in order to comply with the various dissemination limitations. Agencies may already have an inventory of all systems handling CUI information in their FISMA planning or existing FISMA analysis about the data sensitivity levels for each data set. In places where the dissemination rules are consistent across the system, the rules can be implemented through system access with proper vetting procedures. However, in systems that include CUI with different dissemination rules, more fine-grained access control is needed. For each system, agencies should conduct a compliance overview that shows how the system limits the dissemination of CUI to those with the authority for that information. The overview should document any plans for making changes to data access, if required. The following System Inventory Template will help with this review.

System Inventory Template

Data Analysis Template

System	CUI Data Contained	Applicable Safeguarding Rules	Dissemination Rules	Interfaces

System Analysis Template

System	CUI Constraints	All Applicable Safeguarding	Access Controls Available	Interfaces

Step 5 - Plan Development: Many agencies have already begun to consider how they will implement CUI and which office within the agency will be responsible for overseeing this implementation. These decisions will be the foundation of the agency compliance plan. Implementing agency policy is often an extended process; given the time frames required by the Executive Order, these are likely the first step that an agency should consider. Implementing CUI requires an understanding of what CUI is used within the agency and how it will be handled. The systems inventory will define needed technological changes to manage CUI and will likely be a time driver for the total length of time to implement CUI. Training is needed to ensure that agency staff understand the CUI policy. The crucial element of the compliance plan will be the evaluation of each CUI category and your current business processes in using this information. Changes in business process to comply with the CUI categories could have far ranging impact. For example, if the requirements for "acquisition sensitive information" require changes to your business processes, these changes are not just related to security processes but may impact contracts, conflict of interest rules, and other business processes. By thinking through the business process of each CUI category in your agency, the specific details of the implementation plan will become clear. Please see Appendix 2 for a sample Compliance Plan Outline that you can use to build your agency compliance plan.

3.0 | Best Practices for CUI Implementation

The CUI compliance plan is an opportunity to leverage your agency's information assets and enhance your overall security program. For examples of how to do this, we can look to other government agencies worldwide for best practices on protective marking standards and implementations.

The following two examples show how the classification and marking of email and documents can drive more advanced security policies to enhance an organization's overall security program. In both examples, the organizations are using TITUS Classification software for email and documents.

With over 300 military, government, and enterprise customers worldwide, TITUS is the leader in message, document, and file classification and labeling solutions. In the U.S., the solution is used by more than 800,000 government and military employees.

Australian Email Protective Marking Standard

Over 30 federal government departments classifying data with TITUS

Since 2007, all Australian federal departments and agencies have been required to follow the Australian Email Protective Marking Standard. This standard requires that all government-originated email contain protective markings to identify the information's sensitivity. Like CUI, these markings are used to identify and protect sensitive information in a consistent manner across the Australian Federal Government.

The marking scheme is standardized across all government agencies. When sending an email, users are required to select from a pre-defined list of security classifications and categories. This list is common across the entire federal government.

Once a classification and any sub-categories are selected, the protective markings are added to the end of the email subject line. The classification is also stored as metadata in an Internet Message Header Extension (X-header). All agencies apply the metadata in the same way, using a common syntax. This enables interoperability across government agencies.

Presently more than thirty government agencies rely on TITUS classification and safeguarding software to comply with the marking standard, including 90,000 users at the Australian Department of Defence. TITUS ensures compliance by automatically applying visual markings to the email subject line and generating classification metadata in an email X-header. Users simply select the appropriate classification label from a dropdown menu, and the software automates the consistent application of those labels in all emails and documents. Additionally, metadata is also automatically added to help other security technology understand what type of data it is and how it should be handled.

TITUS solutions provide several benefits to the Australian government agencies. Before the email is sent, TITUS can perform several checks to see if the user's selected classification is appropriate for the email content and recipients. For example, if a user selects a classification of "IN-CONFIDENCE" and then tries to send the email to a non-governmental organizational, TITUS will notify the user of their mistake so that they can rectify the mistake before a data breach occurs. If a user attaches a document with personally identifiable information (PII) and then marks the email as "UNCLASSIFIED", TITUS will detect the policy violation and warn the user. The solution educates the user on where the policy violation occurred and enables the user to correct the problem before the email leaves the desktop. By providing immediate policy feedback through customizable pop-up warnings, users receive targeted security education that reduces the chance of inadvertent disclosures.

Rules can also be applied at the server level. The email server can examine the TITUS classification metadata to determine whether the classification exceeds that of the receiving system. For example, if a PROTECTED email is addressed to an email address on an UNCLASSIFIED network, the outgoing email server can detect the problem and advise the sender. Likewise, the incoming email server can reject emails with classifications that exceed the classification of the email system. Other options for using metadata include:

- Using a data loss prevention (DLP) solution to scan for classification metadata and block users from copying sensitive documents to USB drives
- Improving archiving and records management by using classification metadata to make storage and retention decisions
- Automatically applying encryption and digital rights management based on classification metadata

The Australian government's standardized classifications also make it easier for government employees to know how to handle information coming from within the organization and from other government agencies. The classification is clearly identified in the subject line, and the TITUS classification software also displays the classification in the email user interface. As well, many agencies add the classification to the email message body at the top and/or bottom of the email. These visual markings increase user awareness about the sensitivity of the information and encourage proper information handling.

> *"With the TITUS solution, we have confidence that information is being properly classified and that it is staying within our organization when it travels via email. TITUS was the clear winner based on the strength of the offering and the value it delivers."*
>
> ***Mitch Levy, Assistant Secretary, Australian Department of Human Services***

The Email Protective Marking Standard has been successfully deployed across all Australian government agencies.

To ensure a successful deployment, most agencies chose to purchase commercial-off-the-shelf (COTS) classification software like TITUS to comply with the standard. They quickly realized that building their own solution would be time-consuming, expensive, and prone to software bugs. As an email add-on, any solution must work seamlessly with multiple email functions, including reply, forward, distribution lists, meeting requests, and task lists. By selecting a COTS solution, government agencies benefit from a stable, user-friendly product, regular product updates and enhancements, a dedicated product development team, and professional customer support.

Users have embraced the classification standard, finding the TITUS solution easy to use and non-disruptive to their daily work. When users have questions about the classification policy, they can access customized help from within the application. They are also guided into making the correct classification choices, from easy-to-use pick lists to content scanning that double-checks their classification choice. From an IT perspective, the software is simple to deploy and maintain, with most organizations rolling out the software overnight or on a weekend.

By classifying and marking their data, the Australian government is able to gain greater knowledge about the type of data that employees handle day to day. They are also able to significantly strengthen their security program in ways that extend beyond the simple selection of a classification label. With minimal training, government employees have become critical partners in raising security awareness, and identifying and protecting sensitive government information.

Canadian Department of National Defence (DND) Classifies All Emails and Documents

90,000 DND employees classifying data with TITUS

With personnel deployed across Canada and around the world, the Canadian Department of National Defence (DND) faces the challenge of a large volume of highly sensitive information traveling via email and housed in documents. As with most military organizations, DND adheres to a classification system for all communications to determine how information should be handled and who can access data.

DND required an enterprise-wide solution to ensure that emails and documents were handled according to the organization’s pre-determined information classification structure. The team wanted a solution that would seamlessly integrate into their existing infrastructure based on Microsoft Outlook and Microsoft Office and that was simple to use and maintain.

> *“Implementing these products from TITUS has enables us to leverage our existing Microsoft infrastructure and has also proven easy for our staff to use on a daily basis. Classification is and will continue to be a cornerstone of our information security policies and these TITUS solutions help us to reinforce security policy with all of our employees on an ongoing basis.”*
>
> ***Eyad Zorob, Senior Technology Officer, Canadian Department of National Defence***

To meet their requirements, DND purchased and deployed 90,000 licenses of TITUS Message Classification and an additional 13,000 licenses of TITUS Classification for Microsoft Office.

Utilizing TITUS classification solutions enables DND to apply consistent labeling on emails across the organization, contributing to the overall security of highly sensitive information.

In addition, DND is using TITUS classification solutions for mobile devices to ensure proper information protection and labeling on both BlackBerry and Windows-based smartphones. For documents, TITUS Classification for Microsoft Office allows individuals throughout DND to classify Microsoft Office documents, helping to reinforce the value of data and clearly specify how it should be handled.

With national defence and international security a top priority in the current climate, ensuring email and documents are handled properly is extremely important. Using TITUS classification and safeguarding solutions, DND can identify the value of their information assets and ensure that sensitive content is compliant, protected, and safe.

4.0 | The CUI Challenge: Next Steps

All agencies should think about the CUI compliance plan as an opportunity in their agency. Information is truly one of an agency's most important assets. Agencies are entrusted with sensitive information and need to manage that data as the asset that it is. The opportunity to truly build a system within an agency that manages and can leverage this information more robustly is an opportunity that must be capitalized upon.

PKH Enterprises has partnered with TITUS to offer organizations the assistance they need in formulating their complete CUI compliance plan. PKH provides legal, policy, and technical expertise on CUI and can help agencies at every stage of your CUI implementation. TITUS classification and safeguarding software solutions are available in combination with PKH's facilitated training and work sessions to allow organizations to systematically implement CUI.

For further details on TITUS solutions for CUI, download the TITUS white paper entitled "Meeting CUI Requirements with TITUS Classifications Solutions" which illustrates more specifically how you can use a classification management solution to meet CUI requirements.

5.0 | Appendix 1 – Program Checklist

Governance

1. What office is responsible for CUI?
2. How does this office implement CUI policy?
3. Who are the key agency stakeholders in CUI?
4. How does this office communicate to key stakeholders?
5. How does this office address disagreements between stakeholders?
6. How does this office address disagreements between stakeholders and implementers?
7. How is this office staffed?

Policy/Guidance

1. What policies will be addressed at the national level?
2. What policies need to be developed at the agency level?
3. What current policies need to be changed to address CUI?
4. Are there acquisition policies that need to be changed?
5. Are there currently unwritten policies that need to be documented due to CUI?
6. Are there information sharing agreements (e.g., MOUs, MOAS, etc.) that will be influenced by CUI?
7. Are there agency non-disclosures that will be impacted by CUI?

Training

1. Who will need to take training?
2. Should the agency CUI lead manage training or facilitate training through an agency training office?
3. How will recurring training be handled?
4. How will training be tracked?
5. What is the process to address people deficient in training?
6. Are there personnel that need additional training in CUI?
7. Who is in charge of maintaining the “classification guide” for CUI?

Technology

1. Are you including the offices that manage systems and system upgrades?
2. At what level do you want to address system compliance? At the system level or the data level?
3. How many systems handle CUI?
4. Who manages those systems?
5. How will the system requirements be developed? And by whom?

6. How will you track technology compliance?
7. What are your processes before the technology is compliant?

Compliance Program (including Self-Inspection)

1. Does the office managing CUI need to review the procedures for implementing CUI?
2. Does the office managing CUI need to review the physical security of CUI storage?
3. Does the office managing CUI need to inspect marking procedures?
4. Who conducts “self-inspections”? How often?
5. How is self- inspection reported?
6. What is the process for addressing violations? Is there a differentiation between wilful and non-wilful violations?

6.0 | Appendix 2 - Compliance Plan Outline

Agency Commitment - Start the document with a commitment from a senior executive within the agency, describing that the agency is committed to implementing the goals of transparency and information sharing in a compliant form and will therefore implement CUI.

Establishment of a CUI program

This section should describe:

1. Authority – Who will be the lead for CUI in the agency and what are they allowed to do based on what formal delegations of authority?
2. Governance and Coordination – How will the CUI lead coordinate across the internal and external stakeholders of the organization?
3. Training – How will the agency develop, manage, and track training? Who will be required to take CUI training (this should consider: all employees, contractors, and outside partners)?
4. Self-Inspection and Oversight – How will the CUI lead oversee that the implementation is progressing and ensure long-term compliance?

Implementing CUI in the Agency

<u>Approach</u>

This section should communicate the mission drivers that lead to the need to implement CUI in the agency and how they will be addressed uniquely through the agency implementation. In this section, you should also discuss what the minimum requirements are that need to be accomplished before agency handling procedures are changed. For example, does the primary email system need to be compliant before transition? What other key activities need to be accomplished to allow a smooth transition? This section should also address any phased implementation approaches being taken and the justification for those phases. A sample schedule is set forth below.

<u>Sample Schedule</u>

1. Implementation Planning – How long and what are all the steps that will be taken before anyone needs to change their current handling procedures for CUI? Some basic steps include establishing authority, governance, policy and processes, basic technology issues and initial training.
2. Implementation – This is the phase where the employees start to change their information handling procedures.
3. IT Implementation – It is expected that IT implementation will require longer to ensure that efficient implementation is built into other upgrades. Although there may be key systems where CUI would be the driver of an upgrade (such as departmental email systems), other systems are likely to address CUI at the system level until future upgrades.

4. Acquisition Implementation – Another area that is likely to take considerable time to complete is the transition of all contract clauses concerning handling of sensitive information. Although new policy will be applicable to contractors, individual contract updates are likely to be completed over time. New contracts should plan for compliance at the time of execution.
5. Other elements requiring additional time or complexity – Although all agencies are likely to have IT and Acquisition time frames; in various agencies, specific information, such as printed material, unique systems, or emergency procedures may require additional time to complete implementation. These implementation approaches should be described.

Milestones – This section should describe the milestone activities that show ongoing progress in implementation and compliance review.