FORTRA

WHITE PAPER *(Titus)*

Meeting Controlled Unclassified Information (CUI) Requirements

Strategies to comply with Federal CUI Rule (32 CFR Part 2002 and NIST Special Publication 800-171

Overview

Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program defines a uniform policy for the treatment of unclassified information that requires safeguarding or dissemination controls. The CUI Executive Order specifically adopts, defines, and institutes CUI as the single designation for all information formerly designated by Sensitive but Unclassified (SBU), For Official Use Only (FOUO), and other similar designations. This framework standardizes practices around the sharing of controlled unclassified information, with the goal of improving the sharing of information within the executive departments of the Federal Government.

As of December 31, 2017, all federal contracts will require contractors to comply with the Federal CUI Rule (32 CFR Part 2002) that governs the treatment of CUI. These security requirements are defined in NIST Special Publication 800-171, which applies to CUI in nonfederal information systems and organizations.

This white paper looks at important elements of the CUI Framework, and describes how Titus provides the ideal solution for meeting CUI marking and safeguarding requirements.

CUI Framework

Prior to the CUI order, executive departments and agencies used a variety of markings to indicate information related to privacy, security, proprietary business interests, and law enforcement investigations. These markings, and associated policies and procedures, were often ad-hoc and agency specific. As stated in the Executive Order, "This inefficient, confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing."

To address these problems, the order mandates the use of CUI as the exclusive designation for unclassified information requiring additional safeguards and dissemination controls. The National Archives and Records Administration (NARA) maintains a public CUI registry reflecting authorized CUI categories and subcategories, associated markings, and applicable safeguarding, dissemination, and decontrol procedures.

WHAT DOES THIS MEAN FOR FEDERAL AGENCIES TODAY?

Federal agencies should consider the following:

1. Users need to be able to identify CUI in email and documents. This includes adding CUI-compliant headers, footers, and portion markings. The markings should be applied automatically to ensure consistency and compliance with the CUI framework.

2. Any existing marking tools need to support the new CUI framework, and should be able to switch over to the new markings within a very short period. Ideally, the marking tools will recognize the old markings such as SBU and FOUO, and can map them to new CUI markings.

3. Some CUI information will require extra protection such as encryption and dissemination controls. This should be enforced automatically.

4. CUI markings should be stored as metadata, which can be used by downstream technology, such as solutions for archiving, eDiscovery, and data loss prevention (DLP).

5. Any marking solution should be easy to use and require minimal training for the user. Ideally, the solution will be integrated into the user's regular email and document workflow.

Information is truly one of an agency's most important assets. All agencies should think about the CUI compliance plan as an opportunity to leverage, protect, and share this information.

WHAT DOES THIS MEAN FOR NONFEDERAL ORGANIZATIONS?

As of December 31, 2017, all federal contracts will require contractors to comply with the Federal CUI Rule (32 CFR Part 2002) that governs the treatment of Controlled Unclassified Information (CUI). These security requirements are defined in NIST Special Publication 800-171, which applies to CUI in nonfederal information systems and organizations. This means that nonfederal organizations – such as federal contractors, colleges and universities, and state, local, and tribal governments – will also need to identify and safeguard any CUI that they handle.

How Titus Can Help

Titus solutions help federal agencies and nonfederal organizations meet the requirements for marking and safeguarding CUI. With Titus, organizations can:

- Identify CUI in email, documents, and files, and apply CUI-compliant markings and distribution limitations. With support for automated, system-suggested, and user-driven marking, organizations have the flexibility to choose the best approach for their environment.

- Apply special handling rules and dissemination controls to CUI, including recipient clearance checking, redaction of sensitive information, and automated encryption.

- Provide targeted, real-time security education as users work with CUI in email, documents, and files. These alerts and messages increase awareness about the organization's policies, standards, and procedures for protecting CUI.

- Prevent unauthorized and unintended information transfer by applying protection to files where they reside, quarantining files that are stored inappropriately, and flagging files for follow-up where risks are identified.

- Apply metadata to unstructured data so that other security solutions can identify and protect CUI in email, documents, and files. This metadata can be used by existing technology investments, such as DLP, CASB, encryption, archiving, and guards and gateways.

The following section provides examples of how federal agencies and contractors can use Titus to identify and protect CUI.

CUI-COMPLIANT MARKINGS FOR EMAIL AND DOCUMENTS

Titus identifies CUI through a combination of automated methods and human insight, and provides organizations with the flexibility to use the right approach at the right time.

With user-driven marking, Titus prompts users to identify the contents of an email or document before they send, save, or print the information. This causes users to stop and think about the sensitivity of the content, which fosters a culture of awareness and engages users in the organization's information security strategy.

The solution guides users through the marking process, whether through simple dropdown lists for CUI categories and sub-categories, or more advanced classification schemes for classified information (such as the DoD 5200.01-v2 military marking scheme). With a user-friendly interface and customizable online help and help tooltips, the solution requires minimal user training, and is easy to administer.

In the example in Figure 1, the user has composed an email and clicked Send. At this point, Titus prompts the user to categorize the contents of the email.

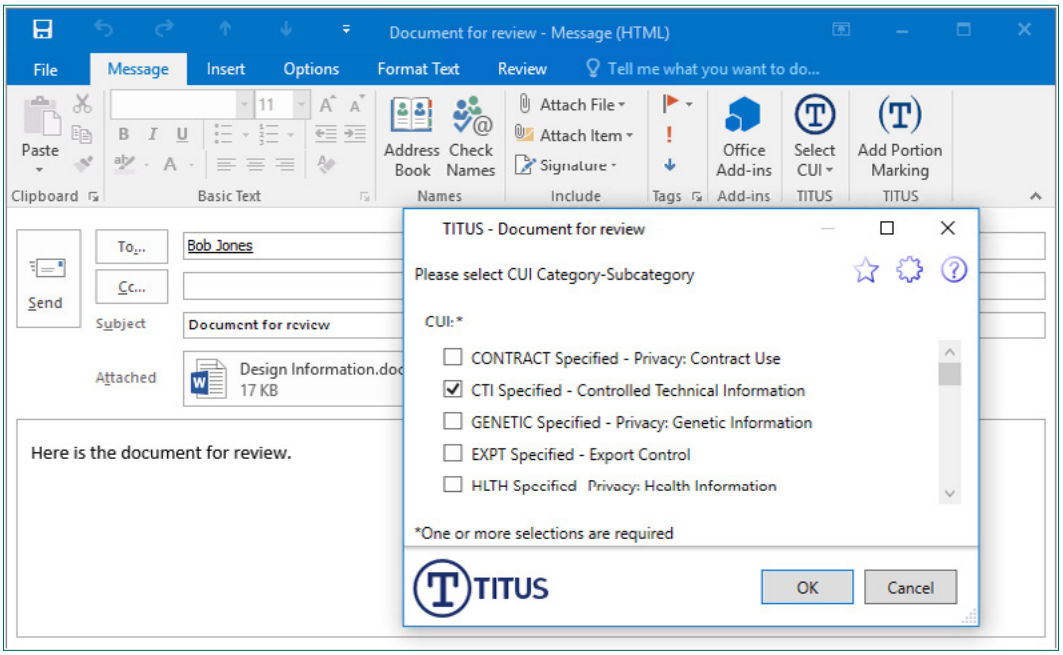

Figure 1: User is prompted to select from a configurable list of CUI categories and subcategories

The format of the CUI categories and subcategories in the user interface is completely customizable. For example, the list could be organized by category and then sub-category, rather than one large list as it is shown in the example above. Or it could prompt the user to choose between “Uncontrolled Unclassified Information” and “Controlled Unclassified Information” before prompting for the CUI categories.

After the user selects one or more CUI categories, Titus applies visual markings to identify that the email content contains Controlled Unclassified Information. These markings increase user awareness about the sensitivity of the information and encourage proper information handling.

Markings are defined by the Titus administrator, and are completely configurable, including control over color, font, size, location, and text. This enables organizations to comply with the specific marking requirements of the CUI registry.

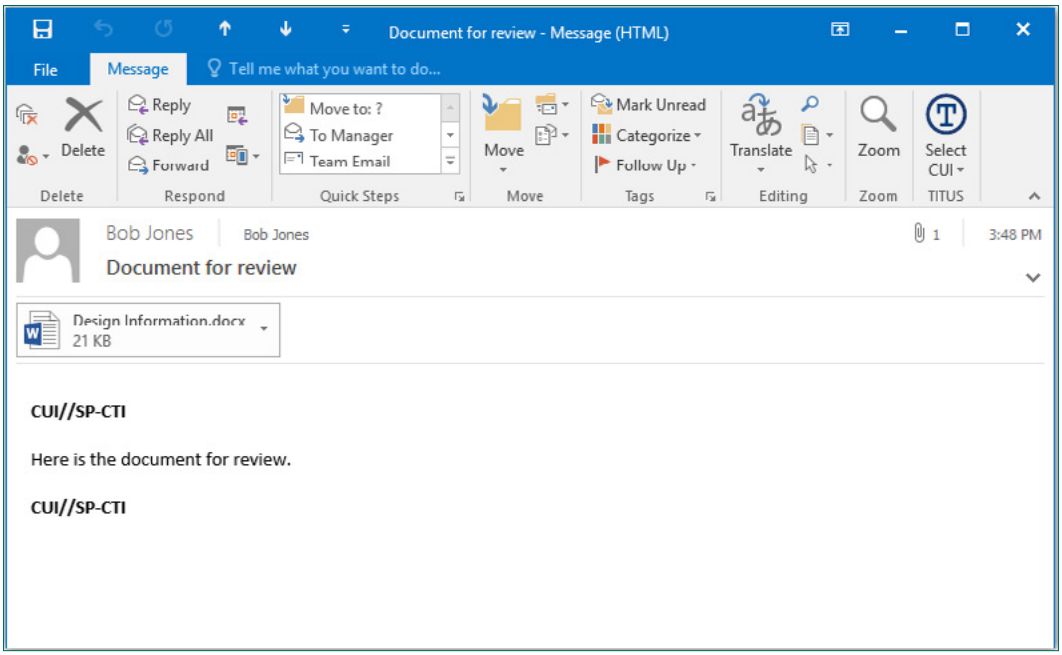

Figure 2: CUI markings are applied automatically

Users can also select CUI categories and subcategories before they save or print Microsoft Office documents. Based on the user's selection (or an automatic selection if that is configured), Titus applies visual markings in the form of CUI banners (headers and footers) as shown in Figure 3.

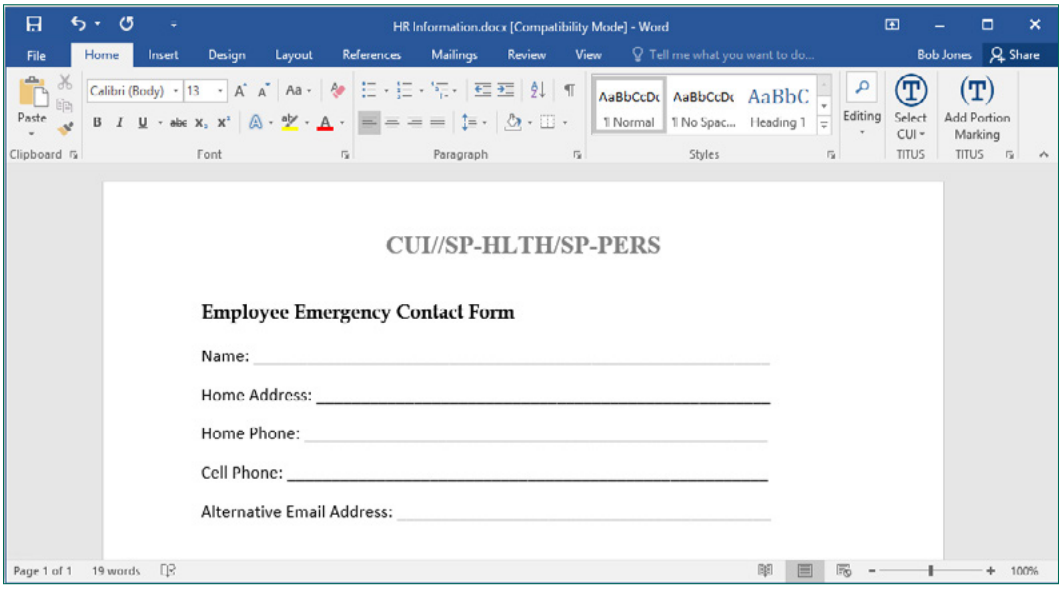

Figure 3: CUI markings in Microsoft Word

Titus also supports portion marking. This feature enables users to mark individual sections of an email or document, such as paragraphs, tables, lists, and subject line. Titus ensures that the markings are correctly formatted for CUI, eliminating the errors associated with the manual application of portion markings.

If a user applies a portion marking that is higher than the overall email or document's marking, the software upgrades the marking to a higher level, and updates the visual markings and metadata to match. This helps to prevent inadvertent disclosure.

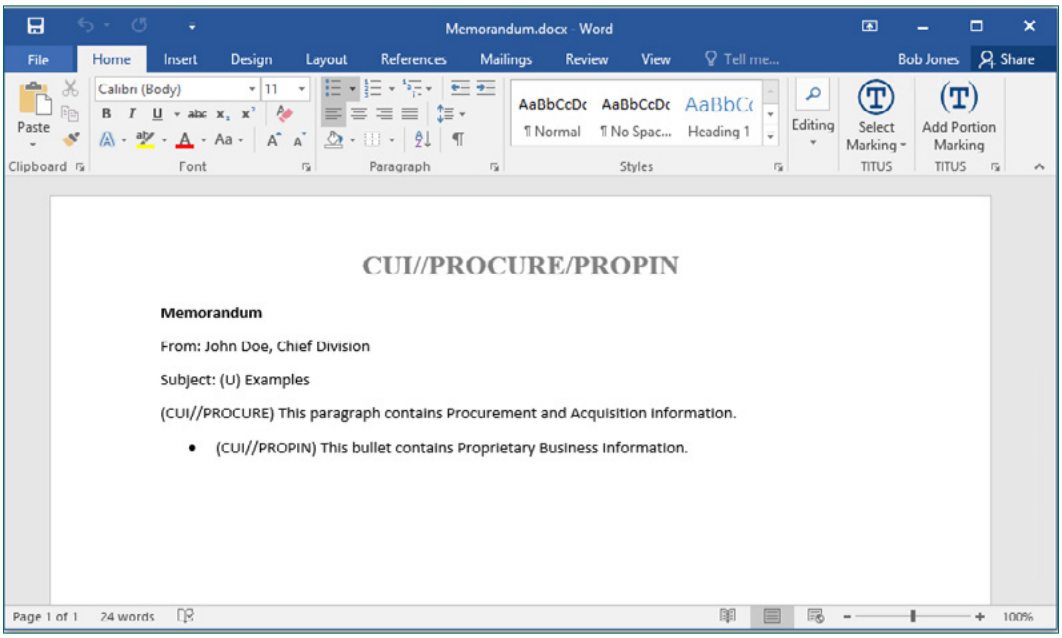

Figure 4: Titus supports portion marking in Office and Outlook

SEAMLESS TRANSITION TO NEW CUI MARKINGS

Titus is designed to easily handle the transition from old markings, such as SBU and FOUO, to the new CUI categories and subcategories. This transition can be handled in several ways.

- **New CUI Categories:** Titus administrators can rename or remove existing categories in the Titus configuration, and replace them with the new CUI categories and subcategories. The next time users launch Microsoft Outlook and Office, the new categories will appear in the CUI list and the old categories will no longer be available.
- **Label Mapping:** Organizations may choose to map the old SBU and FOUO categories to the new CUI categories. If a legacy document or email contains older metadata, Titus can recognize and map it to the new CUI categories. If the user updates the document, or replies to or forwards the email, the new CUI markings will be applied. In cases where mapping is not straightforward, users can be prompted to select a new CUI category when handling previously marked information.

- **Batch conversion:** Organizations may choose to batch convert large numbers of documents, so that documents with old markings (or missing markings) can be updated to show the new CUI markings. Titus provides solutions that enable this process to take place on the user's local machine, in file shares, or in the cloud.

Whichever method an organization selects, the conversion process is simple to set up, and is non-disruptive to users.

AUTOMATIC DETECTION OF SENSITIVE INFORMATION

Titus can be configured to remind users about CUI policy before they send an email. In the example in Figure 5, the user has attached a document that contains personally identifiable information (PII), and has just clicked Send. Titus immediately scans the email and document, recognizes the PII, and warns the user that they need to remove the PII or change the CUI category.

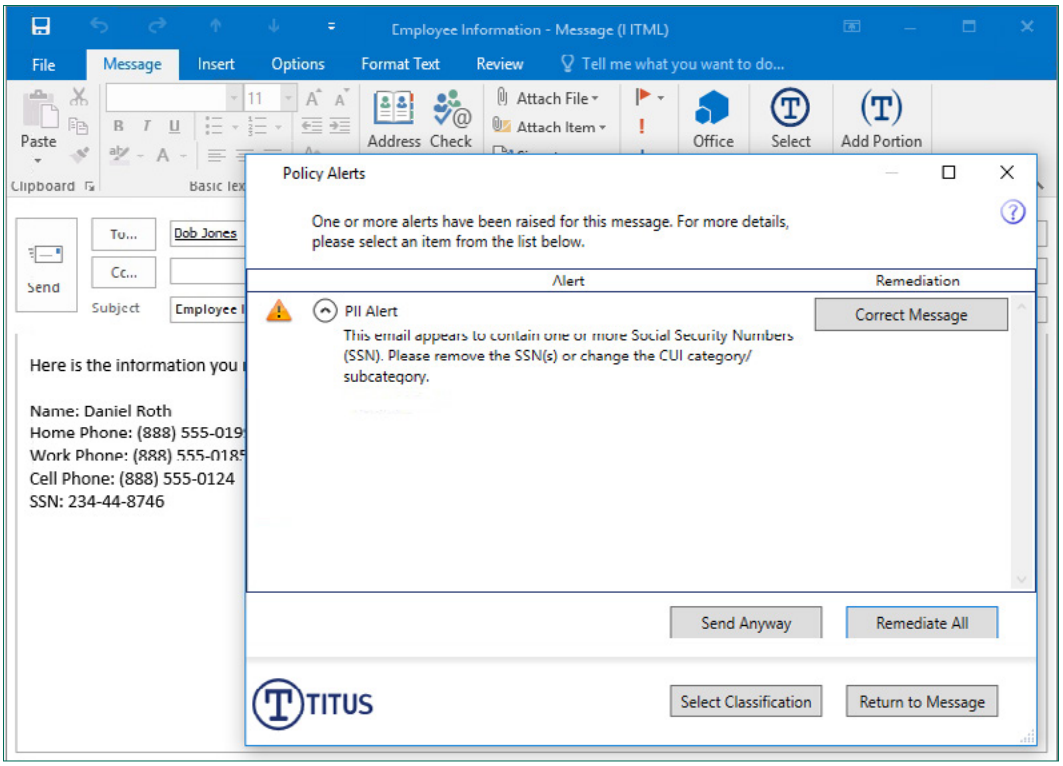

Figure 5: TITUS scans the email for personally identifiable information (PII) before the email leaves the desktop

Titus also provides the ability to redact sensitive content. When sensitive email content triggers a Titus policy warning, users can click "Correct Message" to see the exact areas in the email where the problem exists. Titus highlights the sensitive information and enables the user to either edit the content themselves or automatically redact the content. Users can also highlight the content they want to redact within the email and simply select "redact" from the menu.

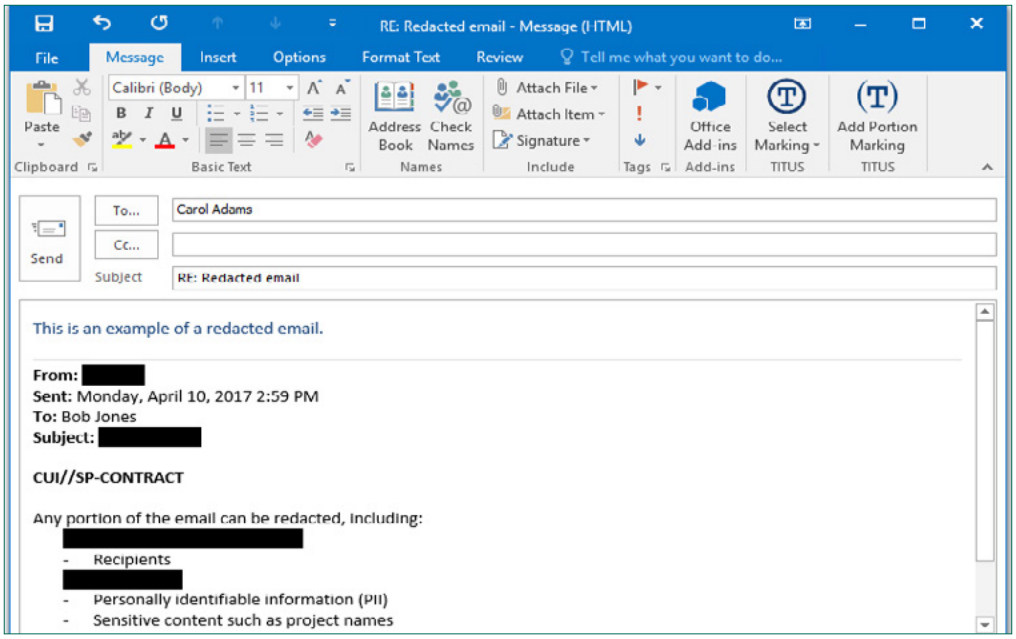

Figure 6: Users can redact sensitive email content

AUTOMATIC SAFEGUARDING OF CUI INFORMATION

After CUI content has been identified, special handling rules can be applied to prevent data leakage. Titus provides several options for this policy enforcement. One option is to use Titus as a front-end to encryption and enterprise rights management (ERM) solutions such as S/MIME, Ionic, and Microsoft Rights Management Services (RMS). Users do not need to understand encryption or ERM; they simply select a label, and the appropriate protection is applied transparently.

Before an email leaves the desktop, Titus can also check the recipients to ensure that they have clearance to receive the information. In the example in Figure 7, Titus uses Microsoft Active Directory to check a user's clearance.

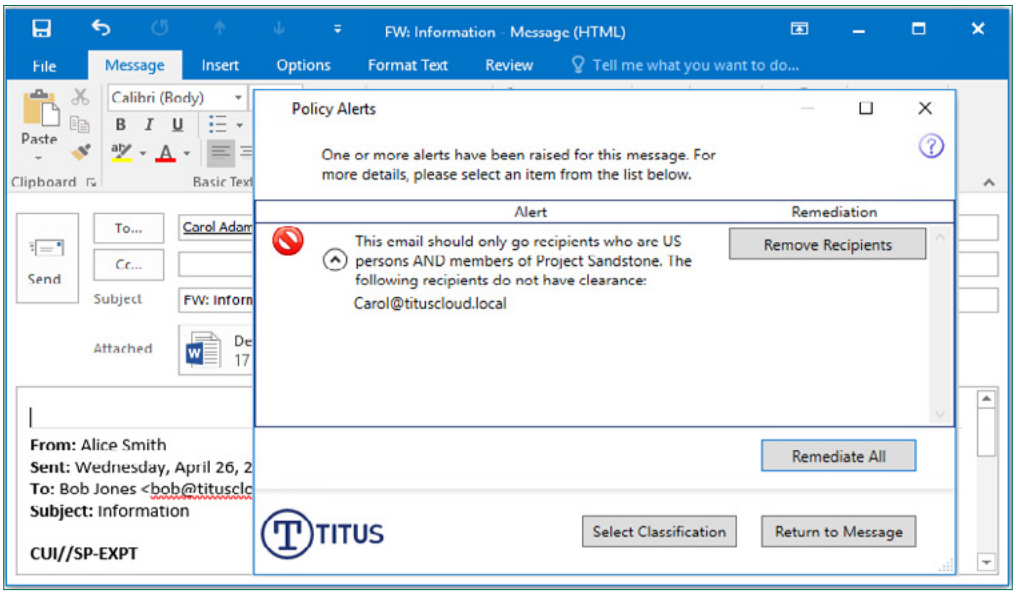

Figure 7: Titus prevents inadvertent disclosure by checking recipient clearance

Titus can also check whether the user is sending email to unauthorized email domains, such as personal email addresses, as shown in Figure 8.

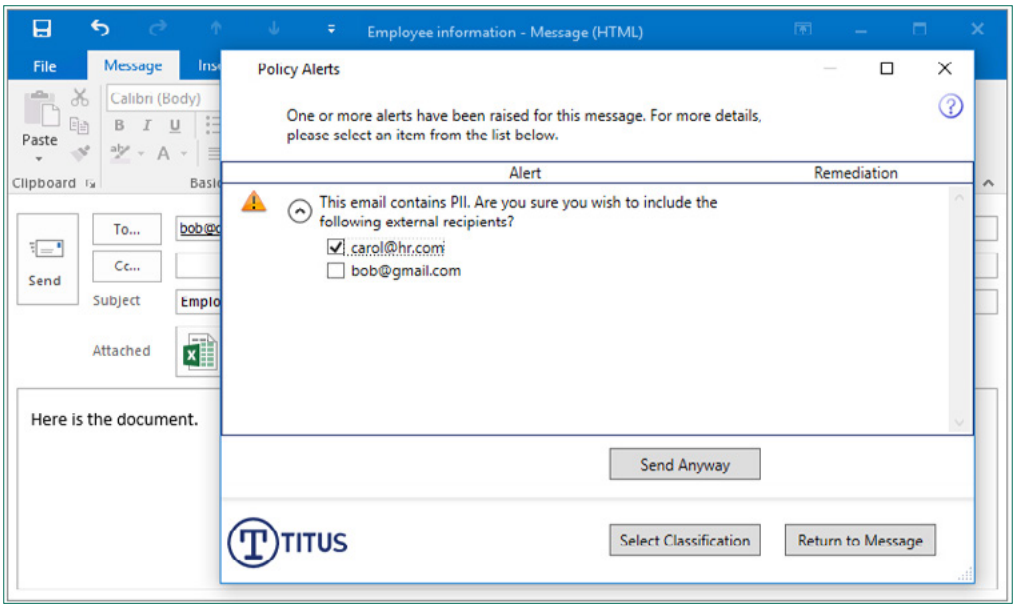

Figure 8: Titus checks email domains and can prompt users to confirm individual recipients before sending

CUI METADATA TO ENFORCE ADDITIONAL POLICY

Visual markings are excellent tools for promoting proper information handling among users. However, much of the value in information marking lies in machine-readable metadata. Titus solutions generate metadata in the form of SMTP X-headers and MAPI properties for email, Microsoft Office custom properties, PDF keywords, Microsoft FCI properties, DLP tags, and other locations for metadata. These standard metadata properties can be read by other infrastructure solutions, including:

- **Perimeter security solutions** that scan for metadata and can block messages of a certain classification/marking level, or encrypt information before it leaves the organization.
- **Data loss prevention solutions** that can use Titus-applied metadata to determine what type of information is in email and documents, and determine how to protect it. For example, a DLP solution can scan the metadata and block a user from copying a document to a USB drive.
- **Archiving solutions** that can make storage and retention decisions based on Titus-applied metadata.

Metadata is also important for interoperability across Titus products. Titus can check the CUI metadata on attached documents and prevent users from sending CUI information in email with a lower CUI level, as shown in Figure 9.

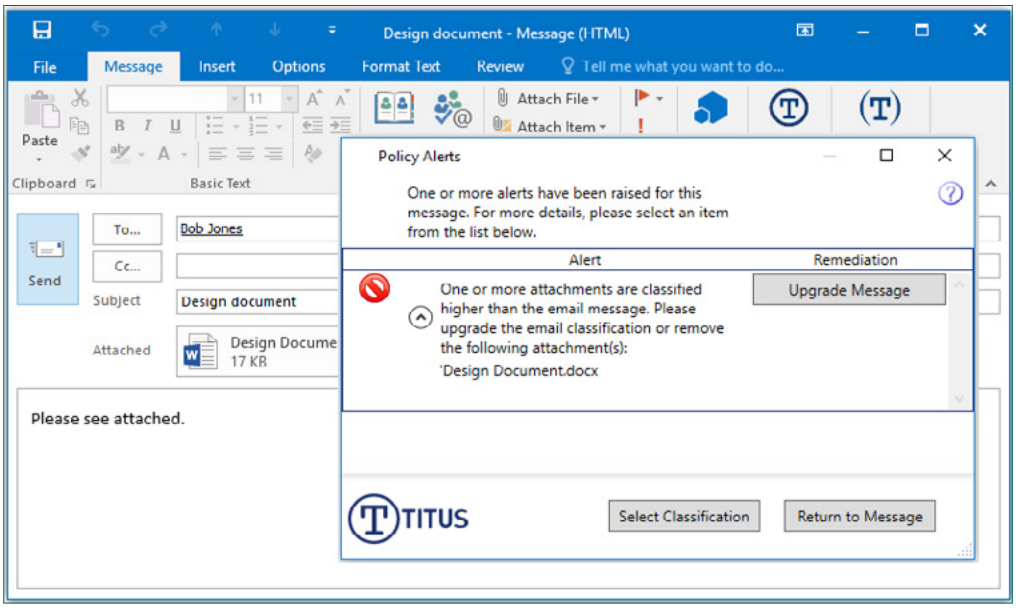

Figure 9: Titus checks email attachments based on metadata, content, and other attributes

Titus Benefits

By using a solution like Titus, organizations can enhance their overall security program and realize the following benefits:

- **Comply with the CUI Program:** The solution enables government agencies and contractors to meet CUI handling requirements as specified in the Controlled Unclassified Information Final Rule and NIST SP 800-171. As a commercial-off-the-shelf (COTS) solution, Titus enables organizations to comply with CUI with minimal impact to internal IT and software development resources.
- **Raise CUI awareness:** The solution adds CUI banners and portion markings in email and documents, helping to ensure consistency and compliance with the CUI framework. These markings raise CUI awareness and encourage information sharing and proper handling of sensitive information.
- **Safeguard CUI from disclosure:** The solution warns users when they are violating policy, such as sending CUI to a recipient who is not authorized to receive it. These warnings provide users with targeted security education and prevent data leaks before they happen.
- **Optimize security technologies:** The solution enhances the ability of other security solutions to protect CUI, including encryption, DLP, network guards, and archiving solutions. By applying CUI metadata to email and documents, Titus makes it easier for other solutions to recognize sensitive government information and apply the appropriate controls.
- **Gain insight into user activity:** The solution can record CUI marking actions and user responses to policy violations. These audit logs can be aggregated into reports that provide insight into information flow, user behavior, and security policy effectiveness.
- **Enhance information sharing:** The solution enables organizations to leverage the CUI framework as an opportunity to share and protect information assets. This helps to promote government transparency while protecting sensitive government information.

Next Steps

Titus has extensive knowledge and expertise in the development and deployment of marking and safeguarding tools. In addition to assisting global enterprises in the deployment of Titus solutions to millions of users, Titus has worked closely with government agencies worldwide to help them comply with data and marking regulations similar to CUI, including the Australian Email Protective Marking Standard, UK Government Security Classifications policy, and US DoDM 5200.01-V2.

To provide additional services to federal agencies moving to CUI, Titus has partnered with PKH Enterprises to offer organizations the assistance they need in formulating their complete CUI compliance plan. PKH provides legal, policy, and technical expertise on CUI. Titus marking and safeguarding software solutions are available in combination with PKH's facilitated training and work sessions to allow organizations to systematically implement CUI.

To learn more about how Titus can help your organization comply with CUI, please visit www.titus.com.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.