FORTRA

WHITE PAPER (Titus)

Using Technology to Aid Classification and Declassification

A Look Inside the Report, ‘Transforming the Security Classification System’

Transforming the Security Classification System – or Why don’t I know what really happened at Roswell?

I will save you the time, the report from the Public Interest Declassification Board will not tell you if we have made alien contact, but it does make recommendations on the use of classification, how and why declassification is important and that technology will facilitate both.

It is important to remember that we live in an age of instant information and communications. Unable to remember who the first Archivist of the United States was? Just Google it! Why should I not be able to do the same for any government document? There are a couple of reasons:

1. You may not have a need to know;
2. The information is still classified; or
3. It is stuck in the approximately 400 million document backlog to be reviewed for declassification.

In its report, the Public Interest Declassification Board runs through the above reasons, outlining:

1. Ways to address your right to know;
2. The fact that it is still classified (possibly unnecessarily over classified); and
3. How to remove that 400 million document back log.

This report is not the solution for all that is possibly wrong with intelligence and military classification doctrine. The board brought together their recommendations after hearing from witnesses spanning all stakeholders in classification and declassification of intelligence and military documents.

At Titus we have had the privilege to work and collaborate with some of the brightest minds in classification employed by the US government and other governments throughout the world. These people agree the current system is not perfect. The current system is a classification system based on keeping national secrets and in-turn their country’s citizens, safe. Individuals are always actively looking for ways to improve the system and at suggestions to make things more efficient. They recognize that in a digital age, the expectations on disclosures are different from when satellites dropped film canisters to be analyzed and a file folder was manila not an icon on your desktop. They, as much as anyone, want to streamline the process.

The current system of classification came about during an analog and paper age. Information was controlled through simple possession. If the file was locked in a cabinet in a secure facility, it was safe. The photographs and film at that time took physical form. The images of the installations were under physical control!

At that time, it was easier to control access to information. It was passed by hand or delivered through couriers. Copies required a physical version of the file or photo and when it was declassified, it was clearly stamped and physically moved to a public archive. In today’s digital world, information begins life digitally and remains digital. Physical possession is no longer required to make copies of files or photos. Declassification is more complex as digital files need to be altered and digitally marked. Multiple copies can reside in many different digital archives. With digital media the question becomes, “is it easier to modify or change?” How can we know which declassified copies have not been changed? Do we know which version is authoritative?

In reviewing the Public Interest Declassification Board report, there are three main areas that are addressed:

The Classification System

The current Classification System was established some 70 years ago, and in the time since has been updated in an ad hoc way. In the early *"…1980s, an increasingly complex national security posture resulted in a sharp increase in compartmented and special access programs."*

The result of this, *"…complexity makes integration and modernization more difficult and worsens over-classification".* The report then outlines six recommendations to improve and modernize the current classification system. The recommendations focus around the move to a two-tier classification system and determination of classification based on risk assessment - on the *"…level of harm anticipated in the event of unauthorized release."* As well, it is recommended that certain information that is *"…information with short-lived sensitivity should be identified and segmented for automatic declassification without further review,"* and that a Safe Harbor clause should be introduced, *"…for classifiers who adhere to rigorous risk management practices and determine in good faith to classify information at a lower level or not at all."* The intelligence community needs better definition, *"..distinguish(ing) between intelligence and non-intelligence sources."*

The board also recommends that, *"The President should appoint a White House-led Security Classification Reform Steering Committee to oversee implementation of the Board's recommendations to modernize the current system of classification and declassification."*

It is an admirable goal of the recommendations to try and be clear on what 'Top Secret' is and what 'Secret/Confidential' is. With the recommended removal of a more stratified top level and the inclusion of second tier Compartmental and Special Access Programs, there will be an increase in the use of Compartmental and Special Access Programs to achieve the same information protection that could have been accomplished at the previous higher level.

In light of the mandate to share more freely across agency boundaries and between different levels of government, it is preferable to have more gradients in the top tier classifications. The more shades at each level, the more continuous and meaningful the overall classification of the information object becomes. This also enables wider sharing of intelligence. If we have only two top levels to classify by, then agencies wanting access to the information will fit into Top Secret/Secret , Confidential, or not at all. Thus you get situations where sharing is necessary and over sharing can happen, or the converse where the need to share is present, but, the gross nature of the top tier classifications does not allow for this particular sharing.

There will always be information that becomes outliers to all other information. This is true for both the least sensitive and the highest level of sensitivity. The concern will always be the outliers beyond the proposed two levels. The inclusion of outliers in the higher of the two levels will diminish the importance of that information relative to the other information classified at that level.

Many times it is not possible to anticipate the level of harm. For example, the classifier may not know what other information the potential recipient of this "unclassified" or "lower classified" information has. It is possible that the anticipated harm will be much more substantial if the person classifying had "perfect information" on what the recipient knows. Unfortunately, information knowledge is often asymmetrical. As way of an example on the possible perils of anticipated level of harm, the earliest indications of something happening in Abbottabad,Pakistan (Location of Osama Bin Laden's safe house) was a tweet noting, "Helicopter hovering above Abbottabad at 1am (is a rare event)". This tweet seemed innocuous at the time, and might be an unclassified type of event under the recommendation. But, taken in context with other information that may have been available at the time (waning moon, frequency of drone activity, @alqaeda following Abbottabad tweets) could potentially make the classification much higher.

The need for intelligence sources to receive extraordinary protection is nothing new. During WWII, the use of German intercepts that where later broken using cryptanalysis of Enigma where designated UTLRA. Today, there are many intelligence sources that are provided additional classifications under 'Top Secret'. Automatic declassification without further review for certain short lived sensitive information sounds good initially. Taken in context of the recent mission to kill or capture Bin Laden, the details of that mission should have been automatically declassified once he was confirmed dead.

There was consideration that the revelation of his capture or death would cause others who could be captured or killed from the information gleaned from the mission to disappear before action could be taken against them. As well, there would need to be time for those who provided the needed intelligence to be removed from harm as well. The simple black and white of automatic declassification is not always clearly defined.

The example presented in the paper of declassifying Desert Storm decision making is compelling and would make for a great read. The declassifying of the leadership decisions made during Desert Storm could illustrate the strong leadership and decisive actions taken by the coalition. It could as well show the decision making thought process and risk/reward judgments made during battle. This information could enable future combatants to avoid certain battle tactics or favor others, as they would be able to use the resulting outcomes from those previous decisions. Unless there had been a significant change in war fighting doctrine or tactics, much of that information could still be applicable today.

The safe harbor provision could facilitate the reduction of over classification. There will need to be standards and gauges created to measure the accuracy of the classification. Taking into account the recommendation on anticipated harm, this becomes much more difficult. Think of the WWII efforts of the America's "Loose Lips Sink Ships", and the British "Keep Mum, she's not so dumb". These slogans implied that even the slightest hint of information was all that was needed to harm allied servicemen. With that in mind, we may not know what anticipated harm may come until sometime in the future.

The Declassification System

Declassification is *"used to remove restrictions on and grant public access to classified information that no longer requires safeguarding". "Because agencies' declassification guidelines and criteria are often outdated or difficult to understand, they can produce inconsistent declassification decisions and missed referrals to other agencies".* This will exacerbate *"…the difficult task of reviewing the enormous volume of these so-called "borndigital" records as they become subject to automatic declassification after 25 years."*

In light of the historical importance of most classified information, there is a pressing need to revamp the declassification. Accordingly, *"…future historians may find that the paper records of early American history provide a more reliable historical account than the inchoate mass of digital communications of the current era".*

The recommendations provided include, *"…Formerly Restricted Data (FRD) information be reexamined."* And *"… would be subject to the requirements of Executive Order 13526, including the provisions for declassification."* As well, *"The President should bolster the authority and capacity of the National Declassification Center (NDC) with specific measures to advance a governmentwide declassification strategy"* and require *"…agencies to share declassification guidance with other classifying agencies and the NDC should be strengthened"* In addition ,*"Historically significant records should be identified and set aside as early as possible after their creation to ensure their preservation, long-term access and availability to agency policymakers and historians". "Agencies should improve records management overall by supporting and advancing the government-wide information management practices".*

One of the interesting ideas advanced is the historical importance of information in classified files. We know that some classified information from as far back as May 1930 involving plans to invade Canada could have been declassified as early as 1955. Imagine the ramifications that could have had on American-Canadian relations at the time? If this information was disclosed at that time, would then Prime Minister John Diefenbaker have maintained his

Throne Speech theme of Canadian interests being placed first with the United States? Would he have established NORAD, canceled the Avro Arrow, built the St. Lawrence Seaway and bought US manufactured Fighters? When it finally was declassified in 1995, it still caused controversy, but seen in modern eyes, it appeared antiquated and whimsical. In the 1950's it could have impeded the increasing cooperation between Canada and the United States.

The provisioning of metadata that provides context would enable a more accurate interpretation of the historical significance of the information to be declassified. This contextual metadata is best provided by the creator of the information, rather then from an exploratory analysis of the contents. The most important aspects of context are not yet discoverable by automated means. Only the user has the history, sources of the information, and feeling for what the intended audiences will want to know about the information being classified.

Improvements in records management is necessary in many agencies. Both the intelligence and DoD community have a proliferation of data. If the records are not managed properly, then the future use in declassifying is diminished. What is not said explicitly is that more contextual metadata will be needed to facilitate declassification decisions.

Where Formerly Restricted Data is involved, the joint management of the information between the Department of Energy and Department of Defense does cause complexity in declassifying this information. The fact that it is excluded from automatic declassification review is also a hurdle to its release. Where this information is no longer mission sensitive or of no operational value, it should be made available for declassification. The historical nature of some of this information (ie. Cold War era) could aid today's historians in better understanding policy decisions made decades ago by elected officials, military leaders and bureaucrats.

The recommendation of applying historical judgment when determining classifications is somewhat subjective. What the recommendation does mention is the use of more data tagging. This additional data tagging could provide provenance of the information, and provide context in which to judge its historical significance.

While an altruistic view is to have the historians assisting those creating and classifying the data, and assisting in the declassifying of the information, the goal of cross-departmental story telling is possibly out of reach.

Using Technology to Aid Classification and Declassification

The previous two sections outline the issues with classification and declassification and what can be done to fix that which is perceived as broken or ineffective. The recommendations in this section point to the solution – the proper use and enablement of classification and secure collaboration technology to facilitate the protection of information and the reasonable disclosure of information after its efficacy is done.

The key recommendation points are as follows:

1. "Automate and streamline declassification and classification processes, and ensure integration with electronic records management systems"

   Titus Message Classification, Titus Classification for Microsoft Office and Titus Classification for Desktop provide automation for classification. Titus solutions allow for the creation of rich metadata that can provide the provenance and context to streamline the declassification. More importantly, Titus classification is done by guiding the users who is classifying the information through the potential complexity of the metadata schema for classification. Titus provides features and functionality to facilitate recommended classification of specific information. Titus products provide visual labels, and add metadata to the information object to facilitate electronic records management systems. Titus also provides security solutions for Microsoft SharePoint that leverage the metadata of the information object with the need to know of the individual accessing the information. This automated policy-based approach streamlines the records management requirement referenced in this report.

2. "Provide tools for preservation, search, storage, scalability, review for access, and security application. "

   Again, Titus software assists in all the areas listed above -- specifically Titus software can assist in the areas of preservation, search, and storage. The rich metadata added to the information object provides context for preservation and sufficient detail for search to determine the applicability of the information object. Additionally, the metadata can dictate if the information object should be stored at all, and if so, what method of storage.

3. "Address cyber security concerns, especially when integrating open source information into classified systems."

   With the proper metadata associated with open source information, cyber security systems can leverage it to make access control, storage, linking and embedding decisions.

4. "Standardize metadata generation and tagging, creating a government-wide metadata registry, drawing on lessons learned from the intelligence community."

   Titus has focused considerable research and development into standardized metadata generation and tagging. The Titus metadata infrastructure provides a standard way to define metadata schema, provides the standardized schema to different information generating systems, and offers a standard way for end users to do classification regardless of the type of information.

5. "Accommodate complex volumes of data (e.g. email, non-structured data, and video teleconferencing information)."

   Titus provides classification solutions for both structured and unstructured data. Titus Classification for Desktop allows for the classification of a variety of file types, and applies standardized metadata which is provided in an easily consumable form to downstream systems.

6. "Advance government-wide information management practices by supporting the President's Memorandum on Managing Government Records."

Titus has always supported a variety of government initiatives for classification of information, and will continue to facilitate the advancement of government-wide information management practices. Titus is uniquely positioned to help achieve these goals through the work of Titus Subject Matter Experts, and the deployed footprint that Titus products have on both the classified and unclassified networks in the US Government.

Conclusion

The report provides strong guidance to both the US Government and to Titus on what the challenges are today. For Titus, this report highlights market needs while at the same time confirming that the current Titus product strategy will meet the classification needs of the US military and intelligence community today and into the future.

Titus products are available today to enable the recommendations contained in the report. The use of Titus Message Classification, Classification for Office and Classification for Desktop can provide the rich metadata and policies to enable more meaningful and relevant classification of sensitive information, and can facilitate its proper disclosure in the future.

While the report didn't disclose if alien contact had been made, it may provide the framework that at some time hopefully in the near future that information may be declassified!

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.