Policies for the Handling of Security Classified Information in International Organizations
By: Marie Shockley, MASLIS
With Ineke Deserno (NATO), Eng Sengsavang (NATO), Shadrack Katuu (IAEA), and Julia Kastenhofer

ABSTRACT

What is security classified information and how do we, as archivists and records management professionals, deal with it? The policies and procedures organizations have, or do not have, regarding security classified information can cause major disruption in access to the information as well as transparency for the organization. My research has focused on developing resources to help staff of organizations that regularly handle security classified information to manage and handle classified information using best practices within a framework that best supports the maintenance and preservation of authentic, reliable, and usable records and the cloud environment. In analysing the access and classified information policies of 15 international organizations, my research team has identified several key areas in which the tensions between security and access are written into the policies. To aid organizations in the development or revision of their policies, my research team has created a checklist for security classified information policies that brings the policies under an archival framework in addition to the pure security perspective that is common in such policies.

WHAT WE DID

- Contacted over 70 international organizations (IOs) to collect their policies for security classified information.
- Received nearly 30 policies from 15 organizations.
- Participating organizations covered a wide range of IOs in Europe and the Americas.
- Once all the policies were collected, we began to compare and contrast the policies.
  - Were there similar sections? Definitions? Provisions?
  - If there were differences, why? (for example, organization context or the age of the policy?)
  - Were there provisions for digital records or cloud storage? Or were they written in such a way to account for changing technology without specifically mentioning different mediums, etc.?
  - How did policies account for records management principles (like authenticity), if at all?

BACKGROUND

A review of literature focusing on the topic of “Security Classified Information” revealed many trends and gaps.

- Focus on government context—in particular, the tension between a citizen’s right to information and the State’s need to protect.
- A big issue highlighted by this literature is weak definitions in policies for frequently used terms.
- Most literature is written from a security or legal perspective.
- The small amount of archival & records management literature tends to center around the declassification process.

RESULTS

Lit review and checklist to be published and made available through InterPARES Trust.

(Screenshot of table created for tracking comparisons, names of organizations have been hidden or blacked-out for their privacy.)

- Considering these policies, current standards, and the body of literature on Security Classified Information (SCI) we began to create a checklist for policy writing that would take into account records management needs and principles.
- Sent a draft to colleagues for comments and suggestions.
- Edited.
- Sent draft 2.0 to participating organizations for comments and suggestions. This included both organization archivists, records management, and security professionals.
- Edited.
- Sent draft 3.0 to colleagues for suggestions.
- Edited.

CONCLUSIONS

There’s still a lot of room for more discussion and research in this area. While there has been a lot of research into government policy, there has been little published about confidential information in international organizations or even private organizations. Most standards and current literature focus on the security and legal perspective, but fail to incorporate records management principles which would aid in the long-term preservation of authentic, reliable, and usable records. Policies which are created through a more rounded perspective, including security, legal, and archival(records management input will be less likely to cause disruption in flows of information creating a more transparent environment for international organizations, their member States, and society as a whole.