InterPARES Trust Project Report

Title :		Security Classification of Records in International Organizations: An Annotated Bibliography
Document type:		Annotated Bibliography
Status:		Draft
Version:		1
Research domain:		Security
Date submitted:		May 5, 2017
Last reviewed:		May 5, 2017
Author:		InterPARES Trust Project
Writer(s):		Ineke Deserno, Eng Sensavang, Marie Shockley, Shadrack Katuu, Julia Kastenhofer
Research team:		Transnational Team 03

Document Control

Version history			
Version	Date	By	Version notes
1	May 5, 2017	M. Shockley & E. Sengsavang	Ver. 1

Introduction

This annotated bibliography was created in order to examine a large range of documents that focus on and discuss policies for security classified information especially in international organizations. The initial search for articles was fairly broad and included government white papers and commission reports as well as articles from security, legal, and archival perspectives. The results can be seen especially in the articles and white papers that discuss 'sensitive but unclassified' documents. Because some of the key issues on this topic are in the definition of 'sensitive but unclassified' and where the line between classified and 'sensitive but unclassified' is drawn (if indeed, there is a line at all) it was difficult to separate the two. However, in the process of research it was decided that this category of documents was outside of the scope of this project and the search was narrowed, though some of these initial articles were left in the bibliography for their rich discussion on what defines security classified information. Though special attention was given to articles discussing security classification in international organizations, the majority of articles found focus on security classification in governments. Because there are so few articles on security classified information in international organization all these government centered articles were included with acknowledgement that though some issues may differ, many would be very similar in both international organizations and governments.

Annotations

1. Adams, Carolyn. "Protecting Classified and Security Sensitive Information." *Reform 83* (2003): 56-61. http://www.austlii.edu.au/au/journals/ALRCRefJl/2003/27.html

Abstract: The Attorney-General has asked the Australian Law Reform Commission (ALRC) to inquire into and report on the protection of classified and security sensitive information, in the course of court or tribunal proceedings, and in contexts such as freedom of information applications - whether existing mechanisms provide adequate protection for classified and security sensitive information - whether there is a need for further measures in this area.

Annotation: This article is essentially a six page summation of the purpose of the Australian Law Reform Commission's investigation "on the protection of classified and security sensitive information in the course of court or tribunal proceeding" (57). The resulting report of this commission is annotated below (#8). Adams article, written before the commission had finished their investigation and report sets up the context in which the commission was formed and brings to focus the commission's goals to investigate what classified and security sensitive information actually is, the consequences of classifying information, and how classified information is used (or not used) in courts and tribunals. Adams, who was a participant in the commission, concludes the overview of the commission's goals by pointing out that substantial

change may not be needed, and that despite the current heightened security concerns, new methods of handling classified and security sensitive information may not be justified (60). It is important, she says, that civil liberties not be "unreasonably curtailed" (60) and that if changes are made, protections "against administrative and executive abuse" (60) must also be introduced. The questions raised in this article and ultimately, by the commission, highlights the uncertainty in many organizations surrounding the processes and policies of classifying and declassifying or reclassifying documents.

2. Aftergood, Steven. "Secrecy is Back in Fashion." *The Bulletin of the Atomic Scientists* (2000): 24-30.

Annotation: Written during Steven Aftergood's time as director of the Project on Government Secrecy at the Federation of American Scientists this article is the first in a series of appeals to reduce secrecy in the US government. The article argues that there has been an overuse of security classification in the government since the Cold War and asks for change in policy in order to create a more open government. He argues that there are three types of secrecy: (1) national security secrecy, regarding information that would harm or damage national security in some way if released; (2) political secrecy, use of classification for political strategy/advantage; and (3) bureaucratic secrecy, which he uses to refer to "unconscious hoarding and withholding of information that characterizes all bureaucracies" (26). The article points out that the 2nd and 3rd types of secrecy are an abuse of the system and that reform must be made. To this end, he suggests three specific actions to be undertaken. The first action is that the authority to declassify should be expanded beyond the creator; he suggests the possibility of a "Security Classification Appeals Panel" (27). The second action follows a similar thought, expanding declassification authority to courts that hear Freedom of Information Act lawsuits. The third action suggested is to disclose the intelligence budget. Ultimately, this article is a reflection on the problems caused by policies and practices that are based on the fears of the Cold War.

3. Aftergood, Steven. "Making Sense of Government Information Restrictions." *Issues in Science and Technology* (2002): 25-26.

Annotation: Written after the 9/11 attacks in the US this article is an interesting follow up from Aftergood about the abuse of confidentiality in the government. This very short article focuses on the overused and under-defined category of classified information referred to as sensitive but unclassified. He argues that "the failure to provide a clear definition...points to the need for greater clarity in government information policy," (26) and that this clarity should be informed by both "legitimate security concerns" and "the

virtues of public disclosure" (26). Further, he suggests that clear guidelines and practices be created for decision making regarding the use of the "sensitive but unclassified" confidentiality designation and ultimately, that even with policies guiding the process mistakes can happen and therefore there should be an appeals process to contest these decisions.

Although short, this article makes clear the tension between the necessity of government classification and the right of information access by citizens. In relation to Aftergood's previous article which focused on the problems with Cold War based policies for confidentiality, this article also focuses on the problems caused by policies created in fear—except this time it is a much more recent fear caused by the September 11th terrorist attacks.

4. Aftergood, Steven. "If in Doubt, Classify." *Index on Censorship* 37, No. 4 (2008): 101-107.

Annotation: Written in response to "the unprecedented growth in secrecy under Bush" (101), this article points out problems caused by too much secrecy and proposes updating classification policies as a possible method of "confronting over-classification today" (103). Problems caused by too much secrecy, according to Aftergood, are 1) "the possibility for agencies....to depart from legal norms" (101); 2) the tendency to "cripple oversight process by diverting limited energy and resource into futile disputes over access to information" (101); and 3) "it impoverishes the public domain" (101). However, he notes, that sometimes there is a genuine purpose for secrecy and the crucial need is therefore a method of distinguishing "legitimate secrecy from illegitimate secrecy" (103). Aftergood proposes that every classification policy and guide in every government agency that creates classified information should be reviewed in an effort to systematically reduce over-classification by the current administration. In conclusion the article notes that not all problems would be solved by the proposed reviews of policy, but that significant impact would be made and by "'draining the swamp' of over-classification, it will become easier to identify pockets of resistance and to focus more closely on classification issues that remain in dispute" (107).

This article pinpoints, very briefly, the reasons too much classified information can be harmful and through its proposal of a review of classification policies highlights the critical role of policies for creating environments of over-classification. However, significantly left out of the proposal is what the review would be looking for in classification policies—what are the parts of a policy that would create a significant impact of the kind Aftergood believes will result and how would they need to be changed?

5. Aftergood, Steven. “Reducing Government Secrecy: Finding What Works.” *Yale Law & Policy Review* 27 (2009): 399-416.

Annotation: This article continues Aftergood's work on secrecy reform by identifying two successful "secrecy reform programs" (401), analyzing why they were successful, and drawing conclusions on how the government can use these examples to move forward towards more openness. The article has four sections which include introducing the topic and problems of national security secrecy, reviewing the general history of reform efforts regarding government secrecy, examining successful reform efforts, and concluding by proposing "lessons for the future" (401). The first section is a restatement of the topics of his earlier articles (annotated above)—including the identification of three types of secrecy and the core problem of detangling legitimate secrecy from the illegitimate. The second section highlights the committees, task forces, and commissions created in the last 50 years to confront the secrecy problem and highlights their ultimately ineffective results; he states in conclusion of this section, "Despite the intellectual firepower brought to bear and the political effort that was invested, very little has changed with respect to classification policy" (406).

Through the examination of two success cases, the Interagency Security Classification Appeals Panel and the Fundamental Classification Policy Review undertaken by the Department of Energy, the author determines four "secrets of effective secrecy reform" (411). These four key points are that reform is best done at an agency level rather than abstract, "government-wide statements of policy" (411); declassification authority is extended beyond the originating agency; experimentation and pilot projects should be encouraged; and strong leadership is absolutely important. By analyzing two successful cases this article addresses a common weakness in his previous articles on secrecy in the government by identifying clear actions to be undertaken for clearing up what he sees as a secrecy problem.

6. Aftergood, Steven. “National Security Secrecy: How the Limits Change.” *Social Research* 77, No. 3 (2010): 839-852**.**

Annotation: This article covers the topic of secrecy in the US government from a very different angle then Aftergood's previous articles. Instead of focusing on what is wrong with the current system, this article highlights the mechanisms that already exist to correct "improper secrecy" (840). These mechanisms are based on the premise that "the secrecy system does not exist in some kind of abstract isolation" (841) and is instead a "bureaucratic artifact that is subject o pressures" (841). These pressures, he argues, "can be harnessed deliberately to achieve specific disclosure goals" (841). The mechanism/pressures include: investigative reporting and unauthorized disclosure, the Freedom of Information Act, inadvertent disclosure, official investigations and congressional oversight, internal executive branch oversight, and positive leadership. It

is interesting to consider how these mechanisms may or may not exist in organizations other than governments and important to think about how they might affect organizational policies for the handling of security classified information.

7. Australia Law Reform Commission. *Protecting Classified and Security Sensitive Information – Discussion Paper 67.* (2004).

Annotation: A commission was formed to identify "measures to protect classified and security sensitive information in the course of investigations and proceedings" (5) and this is the final report on that inquiry. The paper notes that their main challenge as they perceived it "is to develop mechanisms capable of reconciling, so far as possible, the tension between disclosure in the interests of fair and effective legal proceedings, and non-disclosure in the interests of national security" (10). It has three sections. Part A introduces concept of classifying information, the different categories, consequences that flow when info is classified. Part B considers the handling and protection of classified and security sensitive info in general administrative contexts, and the structure, content and enforceability of the PSM (Protective Security Manual) as well as review some administrative aspects of security clearance processes. Part C reviews principles of fair trials, methods in courts and tribunals to determine whether to restrict access to classified or security sensitive info to the public/parties involved, and techniques used by court and tribunals in other nations and if they could use them in Australia.

Of particular interest to the topic of policies for handling security classified information are the proposals made by the commission regarding improvements of content and enforceability of policies, programs for regularized reviewing classified material, and suggestions for automatic declassification. The reasoning and background of these topics are discussed in Part B of the report. The commission notes that most security classified documents need only be classified for a certain amount of time, and after they should be de-classified (or reclassified), however this regularly does not happen. The resulting proliferation of over-classified documents is "not good administrative practice and may contribute to a culture in which classified information is not adequately protected" (89). To ease this burden the commission recommends a hybrid system of regular review and automatic declassification—this kind of system, it mentions, is already followed by the US and Canadian governments (89-92).

8. Bennet, Gill. “Declassification and Release Policies of the UK’s Intelligence Agencies.” *British Intelligence in the Twentieth Century (2002): 22-32.*

Abstract: This study sets out the declassification and release policies of the three principal UK intelligence bodies – the Security Service (MI5), the Secret Intelligence Service (MI6) and Government Communications Headquarters (GCHQ) – in regard to their archives. It sets out the legislative and administrative framework for the release or retention of Intelligence records, and explains that the agencies' declassification and release policies are all based on the imperative of protecting sources and methods. Where their policies differ – for example, both MI5 and GCHQ release records to the Public Record Office, while SIS does not – the reason can be found in the differing nature of their functions and operating methods.

Annotation: The key point of this article is to explain that the declassification and release policies of MI5, MI6 and GCHQ differ because each organization has different functions and methods. In the course of this explanation the article also touches on the tension that exists between security classified information and privacy of individuals/personnel. Although information may no longer need to be considered classified in order to protect the organization or government, it may need to retain secrecy because making it public would impose on an individual's right to privacy. Additionally, the article draws out issues related to processes of review and release—most especially, how slow the process is. Overall, the article stays away from strong arguments for or against current practices, simply attempting to give explanation to why it is the way it is. This neutral approach leaves the reader with several implicit questions to answer. Questions like how different functions and methods can be accounted for in policy, how policy can account for both while still maintaining the principles of accountability and transparency and how can the review and release process be changed for better?

9. Castaner, Gustavo. “Description of Archival Holdings of the International Monetary Fund and the Project to Make Descriptions Available Online.” *Tehnični in vsebinski problemi klasičnega in elektronskega arhiviranja* (2014): 311-321.

Abstract: The Archives of the International Monetary Fund have successfully conducted an ambitious project to produce standardized description of the archival holdings of the institution and make these descriptions widely available online through the use of the software Adlib. This paper will examine the different steps that made this project possible, the lessons learned during the process and the way forward for this excellent project. The views expressed in

this article are the author's own and in no way reflect the views of the Council of the European Union.

Annotation: In the IMF's endeavor to create greater transparency, it was found by external organizations and other stakeholders that having the records available was not equal to access. In answer to this problem, a large project to digitize records and make standardized descriptions available online was undertaken. One of the major issues encountered in this project was in dealing with continued additions to the current descriptions--this frequently occurred as new records were declassified under the new, and changing, transparency guidelines. The process of declassification was "a thorny problem for the IMF given the often confidential nature of the information..."(320) and as a result of this project it was highly recommended that the IMF's current declassification processes be streamlined. A thorough look into how the process might be streamlined and what the impacts of that may be would be interesting for further research.

10. Cosenza, Isabella. “Open Justice and National Security Cases: The ALRC Inquiry into Protecting Classified and Security Sensitive Information.” *Reform* 84 (2004): 50-54, 71**.**

Abstract: Ongoing debate about reconciling the need for open justice and fair trials with the legitimate need for protecting classified and security sensitive information - ALRC's challenge to improve existing system.

Annotation: This article is a review and criticism of the ALRC inquiry (the results of which are annotated above). It notes that the key challenge for the ALRC was "to...improve the existing system, by devising mechanisms (or clearly articulating and consolidating existing mechanisms) that better reconcile the various competing public and individual interests" (50). The author highlights several court cases both in Australia and abroad that demonstrate the issue surrounding the presentation of confidential information as evidence in courts as lead in for explaining the need for a pre-trial mechanism that would identify and deal with he possible disclosure of material in court proceedings. She notes that in the Discussion Paper 67 provided by the ALRC this mechanism would be a proposed legislative Act and shows how similar laws in Canada and the US compare. Ultimately, she is hopeful that the Act will move from proposal to reality as this will aid in the integrity of the system and help insure "fair trials and open justice" (54).

The impact created by poorly thought of mechanisms and policies for handling security classified information are made especially clear in the research exploring tensions between State and individuals in court proceedings, however, these tensions exist in any organization where security classified information is regularly kept. How the individual

right to access information can be balanced with the right of an organization to keep confidentiality is an important question to consider. The mechanisms used by governments may be a good model for other types of organizations.

11. David, James. “Two Steps Forward, One Step Back: Mixed Progress Under the Automatic/Systematic Declassification Review Program.” *American Archivist* 70 (2007): 219-251.

Abstract: Executive Order (E.O.) 12958, signed by President William Clinton in April 1995, dramatically changed the declassification procedure for executive branch records.1 It created for the first time a process to open quickly huge numbers of records dating to World War II. The program has enjoyed mixed success. Many records locked away in vaults for years are finally being reviewed, and, overall, a fairly large percentage of them are actually being declassified. Many high-level documents, however, have been exempted from the process, and major problems hamper public access to the records actually declassified.

Annotation: This article provides a thorough overview of the Executive Orders signed in the US regarding automatic and systematic declassification of records, with particular focus on E.O. 12958 which was the most recent large-scale attempt to create a review program for declassification. The article then evaluates the effectiveness of the program created by this Executive Order, identifying specific problems with the program, and finishes with several recommendations to improve the program and increase awareness/advocacy on the topic of government declassification. One of the key issues identified is the number of exceptions to declassification review—which includes only records National Security Information and Sensitive Compartmented Information, but not information classified under the Atomic Energy Act and only records appraised as permanent in an approved record schedule by NARA.

The article provides seven specific recommendations for improvement of the declassification review program. One, that annual summaries of what has been reviewed, their current location, and when they will be transferred to the National Archives should be made publicly available. Two, "information about all exemptions should be made public" (247). Three, redaction rather than a pass-fail system should be used. Four, NARA should be given more declassification authority. Five, records should be transferred to the NA more quickly. Six, "estimates of the quantities of permanent, temporary, unappraised, and pending-reappraisal classified records" (248) should be made publicly available. Lastly, the NA and presidential libraries need to be more transparent about what has been processed and what has not. Through the seven recommendations it is made clear that author believes transparency of the declassification process to the public is absolutely necessary to a successful review

program. Further, the article argues that not only does more need to be done about the review process, but public awareness of the issue itself needs to be increased.

Highlighted by this deep exploration of the declassification review program created by the 1995 E.O. is the many, and varied, difficulties in either automatic or systematic declassification policies for large organizations with many different functions and, therefore, many different needs regarding declassification.

12. David, James. “Can we Finally See those Records? An Update on the Automatic/Systematic Declassification Review Program.” *American Archivist* 76, No. 2 (2013): 415-437.

Abstract: Executive Order (E.O.) 12958, signed by President William Clinton in April 1995, established an unprecedented declassification procedure designed to release quickly massive numbers of executive branch records dating back to World War II. The program encountered numerous problems, however, and subsequent executive orders pushed back deadlines and created new grounds to exempt records from its operation. Relatively few high-level records have been released and made available to the public. However, modifications to the program made by E.O. 13526 in 2009 and changes proposed by the Public Interest Declassification Board in 2012 will make important progress in reversing this situation.

Annotation: This article is an update written 5 years after the first article, "Two Steps Forward: One Step Back" (annotated above) focusing on developments that have happened since 2007, including the signing of a new E.O in 2009. The first few pages succinctly recount the history and initial problems with the declassification review program that were put forth in the earlier paper. Then the author moves to the 2009 E.O. signed by Obama, which instigated a number of changes to the program including eliminating the deadline aspect and the creation of the National Declassification Center. The article continues its evaluation of the program, stating that is somewhat unclear how successful the review program has been due to a lack of records about the process in the various departments and the lack of standard measurements when quantities of declassified records were counted. The author follows this discussion of issues by summarizing recommendations for improvement of the program that have been made by the Public Interest Declassification Board in a 2012 report. The article concludes that the program has "enjoyed mixed success" (434), with deadlines being continuously pushed back and noting that most records released have only been lower-level. Like the first article, it calls for increased public involvement and understanding. The article is helpful in understanding not only the specific case of the US's automatic/systematic declassification review program, but in analyzing how such programs succeed and fail.

13. Dikker Hupkes, Sander D. “Protection and Effective Functioning of International Organizations.” *Secure Haven,* Final Report of WP 1110 International Institutional Law (2009).

Annotation: This is a report focusing on the legal systems surrounding international organizations, with a particular focus on the Secure Haven project and international organizations (IOs) based in the Netherlands. The report starts with an introduction, followed by three parts: the legal systems of privileges and immunities, legal questions concerning the premises of international organizations in a secure haven, and questions concerning the duty to protect international organizations. These questions are especially framed in order to highlight roles and relationships between international organizations and their host countries. Most pertinent to this annotated bibliography is the introduction in which the definition, classification, and legal status of international organizations is discussed in depth, including the rights, duties, privileges, and immunities of IOs.

Summarizing the definition and characteristics of an IO created by the 2003 International Law Commission the paper points out four main characteristics of an IO: that it is established through international agreements, must between concluded between states and/or other IOs, it must be governed by international law, and must have at least one organ with a distinct will (10-12). Although IOs must share these four traits, every organization is different in many ways; this paper provides multiple possible classifications, by function, according to membership, subject matter, supranational vs. Intergovernmental, and many more. By acknowledging and understanding these many varied types of IOs we can better "analyze the different needs, rights and obligations concerned with the specific categories" (15). In creating policies in an international organization it is important to understand the organization's relationship with various legal entities as well as the functions and purpose of an organization—it cannot be a case of one size fits all.

14. Haight, David. “Declassification of Presidential Papers: The Eisenhower Library’s Experience.” *Provenance* 7, No. 2 (1989): 33-53.

Abstract: In 1972, eleven years after Dwight D. Eisenhower left the White House, archivists at the Eisenhower Library began processing his high-level presidential papers. The library submitted its first mandatory declassification review request to United States government agencies in 1973; sixteen years later this declassification process continues with no completion date in sight. The Eisenhower Library's experience demonstrates that declassifying recent

presidential papers is difficult, expensive, and often frustrating both for the requestor and the library.

Annotation: Somewhat historic in nature, due to having been written in 1989 with direct focus on the declassification review program created by now superseded executive orders, this paper focuses on the practicalities of declassification in the context of a US presidential library. In the program as it existed then, it was necessary that materials be considered page-by-page and therefore all personnel working on the materials had to have TOP SECRET clearance themselves. The program was clearly cumbersome, and as stated in the article, "the mandatory review system involves a large investment of time by library and agency personnel alike" (41). The article asks, "Are there any viable alternatives to the expensive mandatory review system?" (50) and follows with a few suggestions, such as on-site systematic review and increased systematic review from agencies like the National Archives.

The article is particularly interesting to read in combination with James David's 2007 and 2013 articles (annotated above) which also focus on the declassification review system of the US based on executive orders. Together they create a timeline of change in the review system from the page-by-page review based on request described in this article to the much larger-scale program describe in David's more recent articles. Both authors conclude that the program(s) they describe are a mixed success, so one must wonder if a mixed success is 'good enough?' How could these programs be further improved?

15. Hooten, B. Todd. “How Many Ways Can ‘Classified’ be Said?” (paper presented at inForum, Darwin, 2011), available at http://members.rimpa.com.au/lib/StaticContent/StaticPages/pubs/nat/inForum2011/HootenPaper.pdf.

Abstract: This paper speaks directly about classification and declassification of information, but it is not a paper about the process of classification and declassification. It uses these subjects and examples of some policies governing these types of information to bring to the attention of the reader (audience?) some considerations when writing, rewriting or amending policies. It begins with a very brief summation of the United States' classification system under the control of the President and illustrates the difference between "Classified" and "Sensitive But Unclassified" information as well as highlighting the major differences between the policies guiding the handling of these types of policies. Also, there will be examples of how the IMF and The World Bank archives are working together to make things as clear and concise as possible for each other. It is meant solely as a means of making aware some of the benefits of clearly written, consistent policies and the frustrations that can arise due to the lack of harmonization in their design.

Annotation: Drawing on examples from both government and international organization Hooten points out major issues regarding policies for handling classified information. Poorly defined terms, especially regarding terms like "Sensitive But Unclassified" or "Official Use Only" and conflicting or confusing policies within an organization are the main problems explained. Hooten argues that sharing policy information, increased policy instruction for implementation, and "sharing of certain institutional knowledge" (6) would begin to address these issues and should be considered by policy makers.

16. Kastenhofer, Julia and Katuu, Shadrack. “Declassification: A Clouded Environment.” *Archives and Records: The Journal of the Archives and Records Association* 37, Iss. 2 (2016).

Abstract: Declassification is the process of removing restrictions from a record based on the presumption that the information is no longer sensitive. It is a vital part of archival work that has until now been neglected in archival research. The majority of academic journal articles on classification and declassification focus on the political aspects of declassification. Discussions about the mechanics of declassification on the other hand concern themselves with the practical processes of how to declassify information. This article explores the mechanics of declassification in the context of Inter-governmental Organisations (IGOs) in order to enrich the discussion on declassification, politics and mechanics inclusive, by analysing the declassification procedures of five IGOs.

Annotation: This article considers declassification processes and issues in intergovernmental organizations (IGOs) and presents a case study of the declassification procedures of five IGOs. The special status of intergovernmental organizations renders declassification activities in IGOs different from that of state-based organizations. Declassification is part of what the authors refer to as the “records sensitivity lifecycle” (RSL), beginning with classification and ending with declassification. The authors note that “good classification practice includes indicating a date or event when the classification is no longer necessary based on the reasoning that no information needs to remain classified indefinitely” (4). The article refers to Steven Aftergood’s three types of government secrecy: justifiable national security secrecy, political secrecy (classifying for political advantage), and bureaucratic secrecy (classifying for professional or organizational advantage).

The authors identify two types of declassification processes, systematic and ad-hoc. For both, there are six common stages of declassification: trigger, identification of records for declassification, preparation, decision, implementation, and notification (9). In ad-hoc systems, a further step in some organizations may include the appeals process. In their case study of declassification processes of five IGOs, the authors note that all of

the IGOs possess a set of defined exemptions to declassification. The archives play a role in declassification, but that role varies across organizations. The work distribution and authority structures also vary across organizations. In some IGOs, the decision for declassification rests with a committee or with experts in nation state members, while in others, the originating office decides whether records may be declassified. The authors describe various methods for declassification review, but advocate for a risk-management approach based on Greene and Meisner's advocacy for 'use [as] the end of all archival effort' (18). That said, the authors note that declassification is a separate administrative issue from access, and that the two activities are not synonymous. Issues with declassification include its time-consuming nature and difficulties in decision-making, including when exemptions are too vague or too detailed or when records have multiple provenance. Declassification decisions may be based on subject, age or geography. The benefits of declassification include increased access, transparency and accountability.

17. Kosar, K. R. and Library of Congress Washington DC Congressional Research Service. *Classified information policy and executive order 13526.* Library of Congress, 2010**.**

Annotation: This report discusses the history, expenses, and agencies involved in managing United States national classified information policy, focusing particularly on E.O. 13526, the basis for much of the current policy. The report also looks at the Reducing Over-Classification Act issued a year later. The author describes classified information policy as "a range of federal governmental practices that aim to restrict access to information or documents on the grounds of national security" (2). National classified information policy has been established mainly through Executive Orders (E.O) by U.S. presidents (see Table 1, "Executive Orders on Classified Information, 1940-2010," 3), as well as by statutes to a lesser degree. E.Os usually establish who may classify information, the levels and categories of classification, who may access classified information, and declassification procedures. Interestingly, E.Os also prohibit the use of classification on specific grounds "to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security" (4). The Information Security Oversight Office estimates the cost of classified information policy in the billions (see Figure 1, p. 6). The report also notes the distinction between original classification and derivative classification (13).

18. Leyzorek, Michael. “A Missing Feature in Some Records Management Systems.” *ARMA Records Management Quarterly* 32, No. 4 (Oct 1998): 46-48.

Abstract: Many records and information management systems deal competently with the classification and organization of records and provide efficiently for their retrieval when needed and for their ultimate disposition. However, one critical operational requirement of such systems is often overlooked – namely, the protection of the information in those records, during their useful lives, from inadvertent or unauthorized release. Considering that timely and accurate information is a major resource of any organization, the failure to protect that resource from prying eyes is a serious omission. This article deals with this often overlooked requirement of an effective records and information management system.

Annotation: This short article argues that records and information management systems often focus on classification and organization, efficiency of retrieval, and disposition but usually overlook the protection of the information during their “useful life” (46). The author then outlines what he refers to as the “eight steps of information security” (46). These eight steps include determining what information is to be protected (and to what extent it needs protection), identifying who handles the information, defining how it is handled, defining procedures for protection, providing adequate access, balancing the security with operational effectiveness, developing controls and assigning responsibilities, and finally, developing training programs for employees.

In determining which information should be protected the author notes that “the fundamental assumption underlying the classification of any information as confidential, sensitive, or secret is that the release of such information to unauthorized individuals may cause harm or specific damage” (46). He further suggests that the failure of many security systems is defining ‘harm’ too vaguely and thereby classifying too many items. To help this the author suggests asking “what is the nature and extent of the damage, and how serious are the consequences of unauthorized disclosure?” (47) In defining the handling of records he argues the importance of charting specific procedures for “*all* record formats” (47). Though his list of example formats is a little dated he also points out that “electronic media present the most difficult problem because the information stored … is not as easily inspected as that stored on paper” (47). In his conclusion he makes his final argument, pointing out that the people involved are the most important part of information security and that records managers should “point out to company management the relationship between good employee morale and information security” (48).

19. Office of Inspector General, U.S. Department of State. *Office of the Secretary: Evaluation of Email Records Management and Cybersecurity Requirements*. May 2016. Retrieved at https://www.washingtonpost.com/apps/g/page/politics/state-department-report-on-clintons-email-practices/2039/?tid=a_inl.

Annotation: This is a report from the Office of Inspector General created as a response to increasing concerns about "the use of non-Departmental systems to conduct official business, records preservation requirements, and Freedom of Information ACT (FOIA) compliance" (1) of several Secretaries of State in the US. The report reviews the relevant laws, regulations, and policies; assesses the effectiveness; evaluates compliance to the requirements; and, makes eight recommendations for future practice. The report concludes that "longstanding, systemic weaknesses related to electronic records and communications have existed," (42) and "the Department generally....have been slow to recognize and to manage effectively the legal requirements and cybersecurity risks associated with electronic data communications" (42). As a document investigating legality of certain actions undertaken by officials, it does not address the theory or reasoning behind the policies and laws, only if they were followed, and if they were not, why? Consequently, this leads to recommendations that are based on the creator/user experience (namely, more frequent contact between the Office of the Secretary and Office of Information Programs and Services in general, increased and more frequent training, and more briefings on changes) rather than the updating of policy or law.

20. Libicki, Martin C., Brian A. Jackson, David R. Frelinger, Beth E. Lachman, Cesse Cameron Ip and Nidhi Kalra. What Should Be Classified? A Framework with Application to the Global Force Management Data Initiative. Santa Monica, CA: RAND Corporation, 2010. http://www.rand.org/pubs/monographs/MG989.html.

Abstract: For its operational planning and budget programming, the Department of Defense (DoD) needs frequent access to current, detailed data on authorized force structures for all the services. Having users aggregate this information themselves was difficult, time consuming, and error prone. Hence, DoD launched the Global Force Management Data Initiative (GFM DI). While most of the data from the GFM DI are unclassified, the fact that it facilitates data aggregation raised concerns about what a potential adversary might be able to do with access to it and whether it would be better to classify such data and store it exclusively on the secure network. The authors address this question by looking at why material should or should not be classified, concluding that classification is warranted only (1) if it reduces the amount of information available to adversaries, (2) if the information kept from adversaries would tell them

something they did not know, (3) if they could make better decisions based on this information, and (4) if such decisions would harm the United States. Using this framework, the authors balance the risks GFM DI poses against the costs to DoD of not having this information readily available to its own analysts. The authors conclude that overall classification is not necessary but suggest that some limited subsets may warrant additional protection.

Annotation: The article addresses whether a type of military data known as force-structure data should be stored only on a secure network, or whether it could be moved to an unsecure network. In order to answer the question, the author identifies a set of criteria for classifying information, then applies the criteria to the data in question. The study states that "the fundamental rationale behind classification [is] that there should be security benefits from applying it" (8). The author concludes that there are four criteria for classifying information: 1) whether classification "decrease[s] the amount of information going to potential state and nonstate adversaries"; whether "the additional information adversaries would have if it is not classified affect [meaningfully] what adversaries know"; "How likely is this change in knowledge to affect possible adversary decisions (and again, does it do so in ways that help the adversary)"; and whether "the decisions the adversary makes based on such knowledge damage U.S. national security" (xii). The author also notes that it is not always the content, but the context of a document or information that could render it classifiable. For example, information could be classified if it has been supplied by parties who expect the government to keep it secret, or because "how and where the government obtained it is sensitive" (1).

21. Lin, Herbert. “A Proposal to Reduce Government Overclassification of Information Related to National Security.” *Journal of National Security Law and Policy* 7 (2014): 443-463.

Abstract: Lin explores the phenomenon of overclassification in American society and proposes a classification cost metric in order to create serious economic incentives to reduce classification. The metric would provide decision makers with a way to judge the relative importance of different classified documents and allow officials to classify documents on a more objective scale. The author relates a number of questions and answers relating to the underlying approach, the mechanics, budget and finance, and law and policy, thereby parsing out the strengths and weaknesses of his proposal.

Annotation: While many of the articles in this bibliography have centered around declassification, this article purposefully focuses on preventative measures rather than reactive. Citing the same problems as many of the declassification articles regarding the issues with organizations having too many classified documents the author asks how can we reduce "the amount of information that is classified in the first place" (446). This

approach highlights that the problem of overclassification is not one of mere volume, but of creating and maintaining *improperly* classified records (whether due to a mistake in the initial classification or the passing of time reducing/undoing the classified nature of the record). It is unclear to me why an organization would purposefully use the proposed system, as the author states "in traditional economic terms, classification is a free good," (445) so why would they switch to a system in which classification needs to be budgeted? While the incentive of such a system is clear to records professionals, it is not made clear what benefits would be provided for the organization as a whole. In addition, the cost metric proposed by Lin seems burdensome to the record creators, so even if it was implemented in an organization it would likely be difficult to get employees to follow. The system does not seem to allow for partial classification and lastly, the proposed system classifies documents on a kind of 'averaging' system which may allow highly confidential information to go underclassified if the document as a whole was rated 'low' by the system. So, while the idea of changing the system to prevent future overclassification is a good idea, the cost metric created in the article may not be the best way to go about it.

22. Open Society Foundation. *The Global Principles on National Security and the Right to Information (Tshwane Principles).* New York: Open Society Foundations & Open Society Justice Initiative, 2013.

Annotation: This is a set of 50 principles developed to provide guidance for "those engaged in drafting, revising, or implementing laws or provisions relation to the state's authority to withhold information on national security grounds or to punish the disclosure of such information" (5). With the proposed guidance it seeks to strike a balance between the right of citizens to access information and the need for genuine national security. These principles are aimed towards maintaining human rights and dignity at a broad level, but do not provide guidance for practical implementation. Although *some* of the principles do provide notes on 'good practices' that might be used by organizations. The principles are written for governmental organizations rather than international or private organizations and in particular originate from a focus on the state-citizen relationship. However, despite this focus, the principles are still mostly applicable to other types of organizations due to mostly centering on theories and ideas like transparency, availability, public interest, and public safety.

23. Relyea, Harold C. *Security Classified and Controlled Information: History, Status, and Emerging Management Issues*. CRS Report for Congress (2008). Retrieved at https://fas.org/sgp/crs/secrecy/RL33494.pdf.

Annotation: This article traces the history of security classification practices and policies in the United States executive branch, starting from a 1940 directive issued by President Franklin D. Roosevelt, E.O. 8381. According to the author, the origins of security classification are rooted in military practice. The author surmises that E.O. 8381 arose in part from a need to articulate the authority for civilian personnel working in national defense to classify information. Before that, information could only be classified by armed forces personnel. The article describes various developments and changes in policy related to security classification. E.O. 10290, given in September 1951, is significant for three reasons: it strengthened the President's ability to make policy on official secret information; broadened the framework of classified information from reasons of national defense to national security; and extended the authority to classify information to nonmilitary personnel in the executive branch (3).

The management of classified information is defined in Presidential directives, which establish: who is authorized to classify information, the categories of classified information, the duration of classification, limitations and prohibitions, markings and required metadata (identity of classifier, agency/office of origin, date or event for declassification), challenges of classification, declassification procedures, and access to classified information (5).

The article examines differences and similarities between classified information, and different kinds of control markings for sensitive information. The latter include: Sensitive Security Information (SSI), a new control marking for the USDA for unclassified sensitive information; For Official Use Only (FOUO); and Sensitive But Unclassified (SBU). USDA Departmental Regulation 3440-002 of January 30, 2003 describes SSI as "unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity," and outlines types of information that apply (14). Table 1 provides a comparison between the management of Classified versus SSI information. The author concludes that the management of classified information is specified in more detail and clarity than that of SSI, especially in terms of marking authority, duration, prohibitions and limitations, and oversight body (24-25).

The final part of the article discusses challenges in the life cycle management of classified information, including the increased volume of classified information, over-classification, and the costs of managing classified information, which exceed those of declassifying information. For the former, costs include "personnel security, physical security, education and training, and management and planning" (27). Automatic declassification procedures actually help to lighten costs. Table 2 provides costs of classification and declassification from 2001-2006 (28).

24. Roberts, Alasdair. "A Partial Revolution: The Diplomatic Ethos and Transparency in Intergovernmental Organizations." *Public Administration Review* 64, No. 4 (Jul.-Aug., 2004): 410-424.

Abstract: The World Trade Organization and other intergovernmental organizations confront a crisis of legitimacy that is partly rooted in their perceived secretiveness. These organizations have at tempted to address this crisis by promising "the maximum possible level of transparency," but in fact, the improvements have been modest. Policies regarding access to information about intergovernmental organizations' operations continue to accommodate conventions of diplomatic confidentiality. Such conventions are more likely to be breached in areas where disclosure of information is essential to economic liberalization. A true revolution in transparency would require more rigorous policies on disclosure of information held by intergovernmental organizations such as the World Trade Organization, and could be justified as a prerequisite for the exercise of basic human rights, such as the right to participate fully in the policy-making process.

Annotation: Roberts has a large body of work centering around records and information transparency. This article focuses on transparency, or the lack thereof, in intergovernmental organizations, referring specifically to the policies of the World Trade Organization, International Monetary Fund, and World Bank. Rather than debating the minutiae of the policies Roberts examines the habits and culture (the diplomatic 'ethos') that create and nurture policies of confidentiality. From this angle, he is able to exam the possible impact broader transparency in these types of organizations would have on not only the organizations and their participatory nation-states, but on society in general.

25. Schilde, Kaija E. "Cosmic Top Secret Europe? The Legacy of North Atlantic Treaty Organization and Cold War US Policy on European Union Information Policy." *European Security* 24, No. 2 (2015): 167-82.

Abstract: As the EU has expanded its authority into areas of high politics such as monetary, defense, and foreign policy, it has simultaneously developed procedures for handling more sensitive and classified information. These critical policy domains require standards regulating secure information and personnel, but the concept of official secrets is in tension with the treaty norms of the EU. Observers allege that the classified information policy of the EU was imposed through the coercion of external actors such as North Atlantic Treaty Organization (NATO) and the USA in a significant historical departure from the information security policies of European member states. This article evaluates the content of EU-classified information policies and compares them to the

content of European member states, NATO, and the USA, in an effort to clarify the mechanisms of policy diffusion in the area of information security.

Annotation: The article addresses the question of how EU information policy has been influenced by NATO and U.S. information policy. With the widening of EU powers to include domains such as defense and security, the EU has necessarily introduced an information classification system and information access policies for handling classified and sensitive information. Journalists and watchdog groups have claimed that EU information security policy has been unduly influenced by both the United States and NATO. However, the author maintains that the adoption by the EU of information policies similar to those of NATO and the U.S. was less a result of "individual agency" and more the outcome of a number of more nuanced organizational and political factors. For instance, the author observes that EU and NATO nations were already 'coerced' by the U.S. to adopt NATO policy during the cold war, in order to ensure "alliance information security" (168). Moreover, in the early 2000s, due to the EU's increased focus on security and defense, the EU looked to NATO with the aim to increase interoperability and information sharing between the two entities. At the same time, NATO was vetting applicant countries in Central and Eastern Europe, which included ensuring that applicants' information security policies met NATO standards. These factors explain why "the EU currently has the information security regime of twentieth-century NATO" (169). The article continues by outlining EU classification policy and security clearances, and examines the specifics of NATO information security policy.

25. Stephens, David O. "Document Security and International Records Management." *ARMA Records Management Quarterly* Vol. 31, No. 4 (Oct 1997): 69-74**.**

Abstract: Document security defined as any measures instituted to prevent the unauthorized disclosure of confidential, proprietary or otherwise sensitive corporate information, is a small but vitally important area of corporate management and is generally the province of corporate security departments. Yet it is critically important the records managers work with corporate security officials to help protect sensitive information from threats to its integrity due to access by unauthorized persons. Preventive measures for multinational records managers to use include: 1. Attain knowledge of the current document security situation. 2. Communicate with corporate security officials and responsible attorneys. 3. Understand the concept of demonstrable value as the basis for identifying confidential information. 4. Understand the concept of responsible measures for protection. 5. Develop written policies and procedures.

Annotation: Stephens posits that records managers have, traditionally, had very little to do with document security and argues that "it is critically important that records

managers work with corporate security officials to help protect sensitive information from threats" (69). Describing first a case of industrial espionage referred to as the López Affair and several laws related to protection of company secrets, the author then asks, "What can multinational records managers do to help their companies protect their trade secrets or other highly valuable information" (71)? To answer Stephens provides a "*10-step formula*" which focus on communication, developing clear policies and systems, and ensuring employee training and awareness. The 10 steps are clear and easy to understand, if somewhat underdeveloped; for example, step two is to communicate with security officials, but does not provide a clear idea of how to approach these officials or what to talk about beyond the broad scope of "document security" (72). In step five, to develop written policies and procedures, Stephens points out how inadequate most policies are (if organizations even have them) and suggests that many of the key failings would be well-addressed if records managers had been part of the creation.

This article is particularly interesting because it specifically addresses document security in multinational organizations while most research has focused on classified information in governments. Many of the ideas it mentions, like a lack of contact between security officials and records management, are seemingly important but rarely mentioned in other literature and would greatly benefit from more discussion by the profession.

26. Wallace, David A. “Archivists, Recordkeeping, and the Declassification of Records: What We Can Learn from Contemporary Histories.” *American Archivist* 56 (1993): 794-814**.**

Abstract: Over the past fifteen years, the Reviews section of the American Archivist has seen a preponderance of commentaries analyzing guides, manuals, indexes, documentary collections, inventories, and surveys. To a lesser extent, one also finds reviews of texts on archival management, functions, and theory. Although the second of these two groups of writings merits serious and current attention, the former group has been emphasized at the expense of works that can contribute enormously to our understanding of users and recordkeeping systems. This negligence limits our understanding of users, recordkeeping systems, and access issues and minimizes the significance of records as both agent, surrogate, and remnant of human activity and communication. Three recently published volumes from this ignored genre of literature are examined here. These writings contain material relevant to the archival community, and the authors' narratives highlight important archival issues such as access; records creation, destruction, and ownership; accountability; accuracy and authenticity; and document form.

Annotation: This article is interesting in that it appeared in the Re*views* section of the *American Archivist.* Although it does, indeed, review three books it also uses the content of these books to show how the genre can be useful for archivists to read. Specifically, Wallace draws on the experiences of the authors, who had each done archival research and worked with classified records and the systems in place to retrieve classified records, and reflects on them as if they were user case studies—asking, in general, how could we as a profession improve their experience? The author also shows how this genre of non-fiction can add understanding to the historical and social dimensions of archives and recordkeeping systems.

Specifically, in dealing with classified records, the reviewed authors discuss issues with FOIA requests, parallel filing systems, access control, and "subversion of accountability through recordkeeping lapses" (805). The article highlights how keeping records classified unduly burdens the systems creating and maintaining those records but also how it impacts society as a whole by hindering access to and understanding of our past.

27. Yarborough, William Michael. "Undocumented Triumph: Gulf War Operational Records Management." *Journal of Military History* 76 (Oct. 2013): 1427-1438**.**

Abstract: The incomplete nature of operational records generated during and preserved after the Persian Gulf War (1990–1991) has and will continue to challenge historians', medical researchers', and veterans' understanding of the conflict. This war exposed the deterioration of the U.S. Army's records management after the disestablishment of The Adjutant General's Office (TAGO) in 1986. TAGO had overseen Army records management, holding commanders accountable for their units' records and using trained personnel to manage records within units. Focusing on operational records, this paper explores the breakdown of records management during the Gulf War, discusses the presidentially mandated Gulf War Declassification Project (1995–1996), and briefly reviews current Army operational records management.

Annotation: Through a close examination of the US Army's operational records management program during the Gulf War this article illustrates what occurs when an organization fails to have clear policies and implementation procedures regarding records. In the case presented, documents were routinely misclassified (from operational to classified), misdirected, lost, or never inserted into the correct systems. This was made especially apparent when, following the Gulf War soldiers were diagnosed with 'Gulf War Illnesses,' a disease that was traced back to exposure of chemical weapons released at Khamisiyah Pit. The army was unable to "unravel which soldiers were potentially exposed" (1435) due to the poorly kept records. The effort to find or recreate these records through memory in order to identify the movements of all

Gulf War troops cost "thousands of man-hours and millions of dollars" (1435). This processed involved a giant declassification review program as well as many interviews with operations officers in order to rebuild an idea of various unit locations.

The author suggests that if the US Army had maintained pre-Gulf War recordkeeping policies which clearly outlined who was responsible for records and what records needed to go where then the expensive declassification program and interview process would have been unneeded. A relationship between the classification process and the declassification process is clearly implied but not fully explained. It would, therefore, be very interesting to see more research and discussions that link the two processes together and examine the nature and consequences of the relationship.