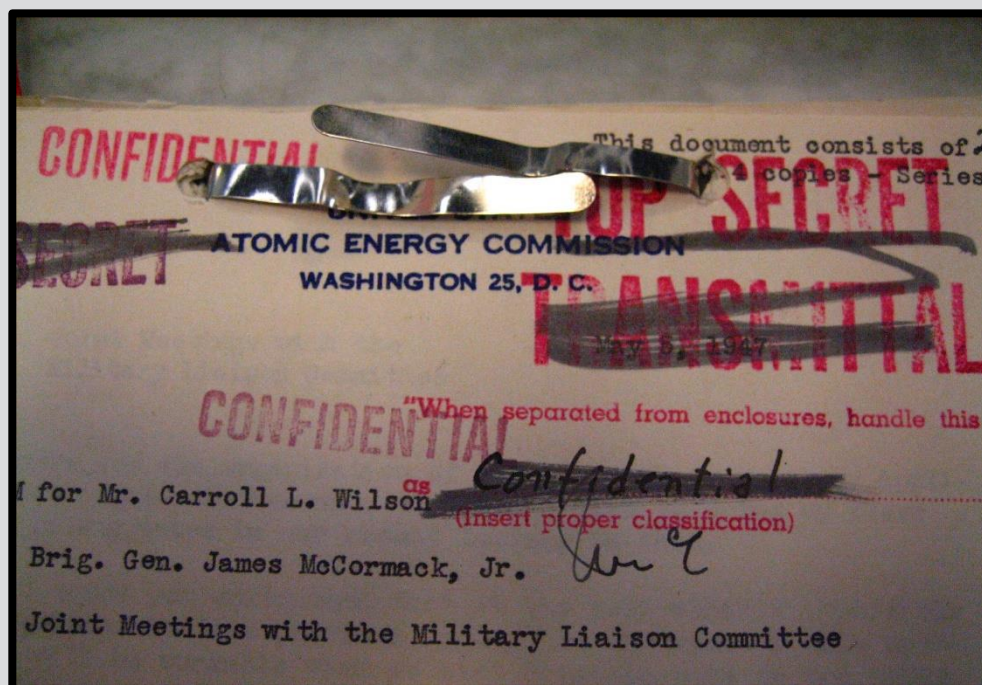


# OCCASIONAL PAPER 2303

## Over-classification: How Bad Is It, What's the Fix?

Edited by Henry Sokolski



March 2023

**NPEC**

Nonproliferation Policy Education Center

Copyright © 2023 by Henry D. Sokolski  
Nonproliferation Policy Education Center  
Arlington, VA 22204  
[www.npolicy.org](http://www.npolicy.org)

Printed in the United States of America

All rights reserved. Except for brief quotations in a review, this book, or parts thereof, must not be reproduced in any form without permission in writing from the Nonproliferation Policy Education Center.

Cover image: Photograph of an Atomic Energy Commission document from the late 1940s  
(credit: RestrictedData via [Flickr](#)).

# **Over-classification: How Bad Is It, What's the Fix?**

*Nonproliferation Policy Education Center  
Occasional Paper 2303*

March 2023  
Series Editor: Henry D. Sokolski

## **Nonproliferation Policy Education Center**

The Nonproliferation Policy Education Center (NPEC), a 501(c)3 nonprofit organization, is a nonpartisan, educational organization founded in 1994 to promote a better understanding of strategic weapons proliferation issues. NPEC educates policymakers, journalists, and university professors about proliferation threats and possible new policies and measures to meet them.

For current publications of the Nonproliferation Policy Education Center,  
please visit [www.npolicy.org](http://www.npolicy.org).

# Contents

---

<b>Acknowledgments.....</b>	<b>2</b>
<b>Over-classification: How Bad Is It, What’s the Fix?.....</b>	<b>3</b>
<b>Why An NPEC National Security Classification and Clearance Policy Reform Working Group? .....</b>	<b>12</b>
<b>Kick-off Meeting.....</b>	<b>17</b>
<b>Increasing Lack of Historical Documentation.....</b>	<b>19</b>
<b>Excessive Secrecy and Cybersecurity.....</b>	<b>28</b>
<b>Space Secrecy.....</b>	<b>33</b>
<b>Keeping Atoms for Peace from Being Overshadowed by Excessive Secrecy.....</b>	<b>40</b>
<b>National Security and Secrecy.....</b>	<b>53</b>
<b>Security Clearances – Barriers to Entry and Innovation.....</b>	<b>61</b>
<b>Are Australia’s Classification Reforms a Model to Follow?.....</b>	<b>70</b>
<b>ITAR: A Security Clearance Barrier to Military Innovation.....</b>	<b>79</b>
<b>How Advanced Technology Can Dig America Out of Its Classification Jam.....</b>	<b>86</b>
<b>How the National Geospatial-Intelligence Agency Controls Its Secrets: The Way Forward for Our Government? .....</b>	<b>99</b>
<b>How Should Congress Manage Staff Access to Secrets.....</b>	<b>112</b>
<b>Working Group Participants.....</b>	<b>121</b>

## **Acknowledgments:**

This project began with a generous discretionary grant from the Carnegie Corporation of New York and subsequently with grants from the Sarah Scaife and the MacArthur Foundations. The project's workshops benefited tremendously not only from the presenters, but the comments and questions raised by the workshop participants. Brooke Buskirk spent many hours formatting and assembling this volume. Finally, a special thanks is due to Golan Rogers who summarized each of the task force meetings presented in this volume and helped develop many of the project's final recommendations.

# Over-classification: How Bad Is It, What's the Fix?

Henry Sokolski

## *Excessive Classification: Seriously Undermining U.S. National Security*

As Donald Trump, Joe Biden, and Mike Pence have all recently discovered, America's national security classification system can catch one out. If these procedures' complexity and murky character merely threatened embarrassment of a handful of high-level officials, though, they might not warrant further attention. Unfortunately, they and their cloudiness threaten far more than that. In specific, their vagueness combined with officials' fear of accidentally releasing – by not classifying or classifying at an insufficiently high enough level – sensitive national security information renders vast and unimaginably large volumes of information, which should be shared at lower classification levels or unclassified, inaccessible. Unfortunately, this over-classification epidemic is killing off our nation's common defense, not protecting it.

Most recently, the Pentagon and Intelligence Community have struggled to make information available to the U.S. public and America's allies about China's strategy to exploit near-space through use of unmanned vehicles and balloons in American, allied, and other nations' air space. Understandably, demand for this information both in and outside of Washington is high.

Meanwhile, the Pentagon decided to improperly use a new classification designation – Controlled Unclassified Information – to keep otherwise public weapons test results from Congress, impairing Congress' ability to conduct oversight. As a result, the Senate Armed Services Committee is questioning the necessity of the marking entirely.

However, the excessive secrecy of high-end classified information, called special access programs or SAPs, is causing great harm to our nation's security and excessively bloating budgets, and reducing our innovative edge. The unhindered proliferation of these SAPs and the lack of oversight and accountability are deeply concerning, as China rapidly develops new weapons systems and tools that we are unable to match in this unwieldy environment.

For years now, senior Pentagon officials (including the deputy secretaries of defense, secretaries of the U.S. Air Force, the Vice Chairman of the Joint Staff, the head of Space Command, the head of the Space Force), our closest allies, and the top aerospace organizations and companies have all complained repeatedly and loudly. Over-classification, they note, has hobbled (and even prevented) important space collaboration with America's allies; protected wasteful, costly programmatic duplications of effort; and significantly slowed rates of

innovation that smaller start-up firms might otherwise fuel. It also has unnecessarily delayed or prevented timely hiring of top-notch, high-tech staff that lack special clearances and cannot get them simply because of artificial 'billeting' limits. It has undermined support for America's most advanced military space programs that might otherwise be available if our diplomats and military could share more of what they knew.

Unfortunately, what over-classification is inflicting against the U.S. military space sector is hardly unique. Military advisors and staff in the Air Force, Army, Navy, and the nation's Intelligence Community voice similar complaints. Each has a tale of military operational dysfunction aided or abetted by over-classification. For example, military units on the battlefield often resorted to using commercial imagery because they were unable to access the excessively classified imagery gleaned from an SAP.

Less tangible but arguably far more important, over-classification has weakened Congressional and Inspectors General oversight and accountability. There are so many SAPs – each compartmented and access so tightly controlled that obtaining oversight access is almost impossible. Congressional staff whose job it is to thoroughly research, gain expertise, and brief their member are almost always denied access to these programs. Only some staff on certain committees are "read-in." While most members are permitted to have a sole staff member cleared to receive Top Secret information, this access does not include SAPs. Even the professional staff on the few congressional committees that are supposed to oversee these SAPs, rarely gain access – and when they do, the limitations and the large number of programs are so extreme that meaningful oversight is almost impossible.

Over-classification has also weakened essential military and diplomatic historical analysis. The Defense Department has long been in arrears in reviewing records 25 years and older. Executive Order 13526, "Classified National Security Information," requires the department and other executive branch agencies to conduct such reviews using specific criteria and keep up-to-date. Its repeated failures have delayed and impacted the publication of Pentagon and official diplomatic histories. These records are essential in understanding our diplomatic, national security, and military history. They are widely used by historians inside and outside of government to make sense of what U.S. officials did right and wrong. Not only do these histories add value to our national experience and reinforce democratic principles of accountability and transparency, but they also serve to aid current policymakers make informed decisions. Unfortunately, the numbers of unreviewed records and electronic data continue to grow at exponential rates.

The Defense Department's failure has also prohibited any historical analysis of highly classified special access programs. These histories – even the classified ones - are essential to help current special access program managers understand what did and did not work in previous programs. Yet, because the Pentagon lacks both "cleared" record managers and



historians and processes to review this information, the histories of these programs are becoming increasingly spotty.

A second classification function – pre-publication review – that could also aid policymakers and help the public gain understanding of their government's performance is also failing. Pre-publication review is a requirement for all staff who hold or held security clearances to submit their manuscript or article for government review before it is published. In theory, this process is meant to ensure that staff does not disclose currently classified information. This process is also required for reports written by contractors supporting various government projects. These reviews are often long-delayed, with higher-level, former officials often skipping the queue and getting to the head of the line. But the decisions also appear to be wanton, with government reviewers requiring redactions or changes even though the information is publicly available. Adopting a risk-averse view that does not appear to actually evaluate whether the information is secret or is publicly available, many government reviewers simply contend that the official would be confirming information that may be classified. These review efforts are so short-staffed, the reviewers rarely conduct research to see what information has been declassified or officially stated. They rarely assess the author's footnotes and instead simply request deletions.

Such bureaucratic caution can blindside Congress regarding programs they must oversee and fund. The Pentagon's embargoing of Controlled Unclassified Information to keep unfavorable missile test information from Congress has already been mentioned. In addition, this year, the Senate hammered out an agreement with the executive to allow one personal staffer per member to view Secret Compartmented Information (SCI) on a need-to-know basis. The House, which is responsible for originating all funding bills, has yet to follow suit. This limitation hinders what members are able to evaluate and assess, including classified briefings on matters they are supposed to oversee.

### *Key Enablers: Too Many Classification Guidebooks and Authorities*

A prime driver of over-classification and restrictive clearance epidemic is bureaucratic caution fortified by too many vague and often conflicting classification guidelines and authorities. No U.S. official wants to be blamed for releasing critical security information to our enemies. But at last count, our government maintains over 2,000 security classification guidebooks (over 400 for the U.S. Army alone) and has granted nearly 1,500 officials with the original classification authority. None of these guidebooks and authorities are the same. Bottom line: If you fail to refer to all of the guides that might be relevant (and too often, even if you do), and proceed to lower or eliminate a classification, you could get caught out, risking your career. Solution: Don't declassify, just say no, then, over classify, just to be "safe."

This works well enough to save one's professional hide. There is only one problem: Too often it harms our common defense (which officials are supposedly sworn to protect). Consider what

happens when American soldiers fighting overseas can't share imagery with allied soldiers to plan a coordinated assault. Or what unfolds when military supplies or intelligence information can't be transferred to friendly states whose help is critical to deter or fight Russia or China? Or what happens when weapons test results, nuclear export information, or civilian plant vulnerabilities that previously were unclassified are kept from the public, Congress, and other authorities?

The answers to these questions are all the same: America's national security takes a hit.

### *The Cure: Consolidate and Automate*

Whenever Beltway insiders hear any of these problems, they almost reflexively throw up their hands and offer a "realism" riff on how all of the incentives are stacked against reforming the system and that "fixing" it is largely hopeless. Even experts who have no direct government classification experience feel comfortable repeating such conventional wisdom. There is, however, one problem with this. This wisdom is wrong. Effective government national security organizations have strong incentives to eschew over-classification, there is an effective way to do it, and it has been done.

About seven years ago, the National Geospatial-Intelligence Agency (NGA) realized it had a problem: The agency was taking way too long to get its images and information to soldiers on the battlefield and when they finally did get this material to them, it was either too late to be useful, or it was classified at too high a level for our soldiers to share it with their foreign compatriots who they needed to plan attacks with on the front lines. In Afghanistan, this encouraged U.S. forces to buy lower resolution imagery from unclassified, commercial sources to "get the job done." Unless NGA lowered its classification, it realized it would lose its customer base to unclassified commercial imagery services.

NGA also recognized that to add competitive value to what it was receiving from other agencies, such as the National Reconnaissance Office, it would have to work even more closely with outside, cutting-edge, private, commercial space service companies. Here, again, over-classification was encumbering such collaboration. The NGA encountered similar problems as it sought to increase its collaboration with close allied governments. In too many cases, over-classification got in the way.

Realizing its future was at risk, the NGA undertook a major review to determine what was jeopardizing its ability to service its customers. During this review, engineer officials discovered that the agency was using 65 different classification security guidebooks. Many were carried over from the legacy agencies that were consolidated into the NGA when it was first created. Most of these guidebooks were created to keep information from being released. In other instances, instructions in the guidebooks were conflicting, vague, or subjective. NGA's

top brass immediately recognized that the classification guides, ostensibly created to protect our national security, were instead impairing it by making it nearly impossible for any NGA official to properly classify or declassify any information or imagery.

To fix this, the NGA's leadership ordered its staff to consolidate the agency's 65 guidebooks into a single book that would give concise guidance. NGA's leadership also directed that in evaluating the necessity and level of classification, officials had to assess if the classification would impair or aid missions and information sharing. Within a mere five months, the consolidation process was complete. In addition to eliminating contradictory, subjective, and vague rules, the consolidation came with clear requirements to review any classification appeal within 30 days and to modify the NGA security classification guidebook five or more times a year based on the outcome of these appeals.

Unfortunately, what the NGA has done is unique. It is quite different than how most of the Pentagon and other national security-related agencies operate. As already noted, the Pentagon alone uses more than 2,000 security classification guidebooks and has over 1,400 officials empowered to classify information and delegate their power to others working beneath them. Rather than update their security classification guidebooks as the NGA does five or more times a year, most security classification guidebooks are reviewed, if at all, no more than once every five years. Moreover, appeals to reverse classification decisions outside of the NGA can take years, not 30 days or less as the NGA requires. In addition, even if successful, these appeals rarely, if ever, result in the guidebooks being modified. These facts are both a symptom of and a catalyst for officials to be overly cautious and to classify almost anything that crosses their desks.

Turning these trends around by getting different national security agencies to use common classification and declassification guides will require a substantial and sustained effort – and driven from the top down, as happened at NGA. In 2012, one intelligence agency indicated it was creating one petabyte of digital data every 18 months. That is the equivalent of billions of paper pages. And that was over 10 years ago. Since then, our national security agencies have created exponentially more data on a wider variety of platforms. Managing this data effectively to support our national security is also increasingly a challenge as executive branch agencies have done little to develop metadata standards and other means to aid accounting and retrieval.

At the same time, our government is hopelessly behind in declassifying even 25-year-old secrets. In 2016, the Information Security Oversight Office (ISOO) reported to the President that the declassification system “remained a resource-intensive, paper-based review process unable to meet the demands of a large volume” of records. Even then, the reviews were ineffective, with only 55 percent of records reviewed actually declassified. In that same report, ISOO highlighted the discrepancy in funding: Over \$18 billion was spent on the classification system while only \$100 million was spent on declassification. Given these facts, it is

impossible to see how our government will ever be able to tally or review what it's doing or has done unless it automates processes.

Recognizing the need for automated solutions to improve classification (and declassification), the Department of Energy tasked its research laboratory to develop a program that uses machine learning technologies to scan documents and assess how or if they should be classified. This effort, however, is quite small (roughly \$10 million a year) and only includes a small fraction of the information the Department of Energy creates. While laudable, the Department of Energy is ignoring that the most significant advances in this technology are being developed in the private sector.

An even greater limitation, though, is that no automated classification-declassification system can ever hope to add value, no matter how good it might be, if it must reference so many different classification guides, especially if they are contradictory, subjective, and vague. In fact, many have highlighted that the use of automated tools without classification and declassification guidance reform will make a bad situation much worse. Reference enough vague and contradictory guidebooks and you end up classifying everything – i.e., replicating the very problem automation might otherwise solve.

The good news is that key parts of the executive branch understand many of these problems and know what is required to fix them. In fact, over the last decade, the number of security classification guidebooks has slowly declined, just as the number of original classification authorities has. Executive branch interest in automating classification and declassification has also increased. Last year, President Biden informed agencies that it was time to replace Executive Order 13526 – the order that governs the classification and declassification system. At that time, this order was 13 years old and his administration recognized the necessity for modernization to better support national security missions and improve accountability, oversight, and public transparency. Still, dedicated funding and strong interagency leadership are needed and cannot be assumed.

### *What to Do*

To catalyze executive action to assure classification and declassification are performed to encourage needed collaboration and cooperation with private industry and allies and to increase innovation and acquisition rates, Congress needs to act. Last year, many congressional members expressed their displeasure with the classification system writ large and with individual aspects of the system. Several members expressed frustration over the ever-expanding costs of special access programs and questioned their effectiveness, given that the information was so tightly controlled that these programs did not support national security missions as they should. Senators weighed in on the need for each Senator's office to have one person cleared to access sensitive compartmentalized information (SCI) to improve oversight.

This year, the Senate Armed Services Committee expressed its displeasure on how the Pentagon is limiting congressional access to Controlled Unclassified Information by asking for a report. Other individual members have complained about the executive's unwillingness to show them copies of the key documents seized from Mr. Trump's estate and President Biden's office. Individual members have complained about excessive secrecy on other matters, such as China's near-space strategy and its recent spy balloon overflight of the United States. They also highlighted the Pentagon's decision to classify the U.S. Government's Space Strategy, noting that this action hobbles an "all of government" approach and effectively limits innovation from the private sector. Other members express both bewilderment and exasperation that the CIA still is unwilling to declassify over 3,000 records relating to President Kennedy's assassination over 50 years ago.

All of this is healthy and helpful. It's not, however, systematic. Although the House Select Committee on Intelligence has an Intelligence Modernization and Readiness Subcommittee, it is unclear how engaged, if at all, the subcommittee is on classification and declassification reform. Meanwhile, the Senate Select Committee on Intelligence has no subcommittees at all relating to this matter.

Ideally, the House and Senate should create intelligence subcommittees focused on the modernization of clearance, classification, and declassification policies. This may be difficult, however, as the congressional intelligence committees (and all committees for that matter) are protective of their turf and privileges, which clearly include their relatively exclusive access to highly classified information. This, then, suggests the creation of a select committee on classification and clearance reform. Unfortunately, however, creating a select committee would be even more difficult to achieve politically than creating clearance, classification, and declassification intelligence subcommittees.

In lieu of these "ideal" solutions, Congress still has an option: It could use the board it created in 2000 to support the oversight and legislative functions of Congress and the policymaking role of the executive branch regarding classification and declassification. That entity – the Public Interest Declassification Board – consists of distinguished citizens with expertise in diplomatic and intelligence history, technology, and classification and declassification processes (as many once held leadership roles at national security agencies). They are appointed by the Senate's and House's majority and minority leaders and by the President of the United States. It is staffed with a handful of detailees from the National Archives and Records Administration, holds regular hearings and meetings, reports annually to Congress and periodically to the President on ways to reform current classification and declassification policies and processes. They have consistently recommended the use of technology to automate classification and declassification processes. Congress has not provided the PIDB with a line-item budget of its own.

The PIDB has already issued several ground-breaking reports, including a 2008 report that led to important policy changes in EO 13526. More recently, it made the case for abandoning paper-based processes to one that uses advances technologies and aligns with digital government. Congress has yet to act on that set of recommendations. Actually, Congress has only sporadically used the PIDB – asking it to review specific classified records and make recommendations to the President on the necessity for their continued classification. Ironically, these requests and the labor-intensive processes they have entailed have only further reinforced the PIDB's view that a radical, new approach to declassification and classification is needed.

To take this on and the more serious role of supporting Congress's oversight and legislative functions, though, the PIDB needs a staff and budget of its own. This Congress has yet to supply. Early last year, the PIDB [wrote](#) Congress asking that it appropriate funds for staff and its operations. The Senate Minority Leader and the Democratic Whip were briefed by the PIDB and agreed to honor the board's request. The Senate Select Committee on Intelligence authorized a budget and independent staff for the PIDB. Unfortunately, the omnibus bill that Congress passed failed to include an appropriation.

Congress should revisit this in 2023. If it did, it could instruct the PIDB to support specific tasks related to classification, declassification, clearance reform, and more. It could task the PIDB with making recommendations to improve declassification of historical retrospective projects like the history of the Afghanistan War. These projects would help Congress execute its oversight and legislative functions and assist it in improving our national security policies. Specific requests could include asking the PIDB to:

1. Determine how many classification and declassification guidebooks various agencies of the government are currently using as well as how many original classification authorities and delegated authorities each agency has. Ask the PIBD to track these numbers annually.
2. Recommend new actions in which different agencies might consolidate their classification and declassification guidebooks and reduce the number of original classification authorities. Ideally, this would result in guidebooks for specific national security missions rather than individual guidebooks for specific agencies.
3. Survey what is being done within the U.S. government to develop advanced technologies to use in automating classification and declassification. It could task the PIDB to compare these efforts with others in the private sector. Recommend how Congress and the executive branch should contract competitively with the private sector to develop such capabilities.
4. Recommend substitutes for using declassification guides – i.e., clarifying when automatic declassification is safe and warranted.

5. Direct the executive branch to track and manage what it classifies, who made the declassification request of whom, what the classified document was, and how many appeals have been made to lower classification or to declassify the document.

Congress could assign the PIDB additional oversight tasks. The aim would be to use the PIDB as a kind of super-competent classification, declassification, and clearance policy Government Accountability Office. To keep the spotlight on the PIDB and the congressional taskings it receives, it also would make sense to create a Congressional Classification and Clearance Reform Caucus consisting of members most interested in these issues. In time, Congress could, then, consider creating a separate select congressional committee to assume oversight of these matters.

# Why An NPEC National Security Classification and Clearance Policy Reform Working Group?

Under a discretionary Carnegie Corporation grant and with additional support from the Sarah Scaife and Mac Arthur Foundations, NPEC held a series of 12 National Security Classification and Clearance Policy Reform Working Group workshops to assess the U.S. government's self-defeating inclination to over classify critical national security information and to determine what can be done about it.

NPEC's National Security Classification and Clearance Policy Reform Working Group consisted of early, mid-career and senior officers and staff from the military, Pentagon, Intelligence Community, Department of State, Government Accountability Office, National Archives and Records Administration, and the U.S. House of Representatives and U.S. Senate. The working group also include senior retired officials, outside government advisers, academics and legal scholars, and other policy experts. The group has close working ties with the congressionally created federal Public Interest Declassification Board (PIDB). Not only does NPEC work closely with the board's staff, nearly the entire board, including its chairman, have participated in working group meetings.

The group examined how over-classification has throttled fulsome analysis of America's most important past military strategic decisions, dramatically slowed rates of military innovation, increased the barriers to competition on important national security projects, discouraged allied and domestic dual-use and defense firms from offering their best ideas and technologies for fear of losing the right to export them to others, seriously undermined achievement of our nation's military space missions, subverted the intent of our nuclear nonproliferation export control laws, prevented Congress from conducting effective oversight and management of the executive branch's most important national security programs, and made it nearly impossible to secure needed cooperation from the private sector to make our internet systems more secure against cyber attacks.

The group also investigated what can be done to reform our classification and clearance systems. These working group sessions included meetings that focused on how Australia's efforts to reduce classification have made their defense and diplomatic efforts far more efficient and what the Department of Energy is doing to develop machine learning to assist in the declassification process. The working group also examined how the U.S. National Geospatial-Intelligence Agency (NGA) reduced the number of classification guidebooks it was using from



65 to one and instituted a system of routine and speedy appeals that could serve as a model for other intelligence and national security offices.

What animated these workshops was the concern that our government's reflex to over classify is undermining the ability of our government's national security agencies to secure the best people and firms, increase critical innovation rates, shorten acquisition timelines, and afford our allies the information they need to work closely with and trust the United States. In addition, the working group recognized that there are growing concerns that over-classification is jeopardizing effective congressional oversight of the Pentagon, Foggy Bottom, the government's nuclear-related agencies, and the Intelligence Community.

How did we get here? It didn't happen overnight. It took decades. It got under way in earnest with World War II and the bombing of Hiroshima and Nagasaki—two nuclear attacks that convinced Washington and the world that pulverizing an adversary's military, political, and industrial centers was the key to killing a nation, winning wars quickly, and deterring future conflicts. Area bombing raids during World War II experimented with this concept; destroying Hiroshima and Nagasaki with nuclear weapons validated it.

After America's nuclear use against Japan, launching, defending, and deterring nuclear air attacks became our military's top priority and a major governmental organizing principle. The United States amassed tens of thousands of nuclear warheads, thousands of long-range missile delivery systems, fleets of bombers, national air and missile defense systems, and dozens of submarine ballistic missile boats. Beyond this, emergency powers were enlarged to authorize military nuclear strikes, to establish national civil defense programs and emergency communications systems, and to build protective bunkers that prioritized sheltering the nation's leadership from the "Day After."

To support these efforts, officials resorted to unprecedented levels of secrecy. Not just sensitive national security government documents, but the discussion of entire topics (such as anything to do with nuclear energy and weapons) were automatically restricted as being "born classified." America's justice system, meanwhile, adopted the policy of making a broad swath of information ("state secrets") too sensitive to be admissible as evidence in legal proceedings.

The unspoken assumption behind all of this was that planning for the worst scenario was smart since all other national security threats—a war on terrorism, regional wars, or similar—were "lesser included threats" (headaches that could easily be taken care of and subsumed by proper preparation for a general all-out nuclear war). Certainly, with September 11, 2001, Washington doubled down on the idea that the common defense required high levels of secrecy.

Today, though, this doubling down rests on shaky ground. Why? Because the world is transitioning to new forms of warfare that can enable states to use high technology to "kill" other nations (or threaten to do so) by targeting their will to fight, rather than by massively

pulverizing their military, industrial centers, and political capitals. This attempt to shift to disabling nations with high-tech systems without physically decimating them is not a “lesser included threat” but something new.

In lieu of threatening physically to blow up most of an adversary's military or industrial capabilities, nations now are competing to unplug and scramble one another's ground and space-based eyes, ears, voices, and nervous systems, all of which are essential to maintaining control over a nation's military and its financial, logistical, and political centers. More important, countries are trying as much as they can to do this without resorting to explosives (using instead robot satellites, electronic warfare systems, lasers, disinformation, and cyber weapons). Nuclear weapons acquisition and modernization efforts (note Chinese, Russian, American, British, French, Israeli, North Korean, Indian, and Pakistani) of course continue, but it would be a mistake to focus only on these developments to understand the strategic trends ahead.

Meanwhile, kinetic warfare is itself transitioning from inflicting indiscriminate, wanton destruction to hitting targets with precision (including Russian missiles aimed precisely at particular hospitals). Further development of these new systems—intelligent, autonomous missiles, drones, submersibles, underwater sensing and processing systems, robotic naval craft, secure communications, and cyber weapons—promises to reduce the prospect of total, industrial-scale wars (nuclear or non-nuclear). These new systems can only do this, however, if they are fed a steady diet of timely, accurate intelligence and relevant data, and only if they are part of public policies and military doctrines that are convincing to both friends and foes.

In this brave new world, less secrecy, not more, will be needed to deter, dissuade, and effectively bargain with hostile states and non-state actors. Washington will need more clearly articulated declaratory military deterrence and retaliatory policies; more demonstrated, quick rates of military innovation and acquisition; and significantly more sensitive information and intelligence sharing with private firms, allies, and friendly states. This does not mean eliminating secrecy but, rather, establishing the right amount of secrecy at the right level—and no more.

Senior officials currently working on America's military space requirements understand this. They are striving to eliminate the yoke that excessive secrecy has burdened them with. America no longer is uncontested in this realm. China, Russia, Europe, Japan, South Korea, India, and Israel all now have moon or Mars missions of their own. Commercial space firms now supply needed communications and multispectral imagery services to militaries, while commercial and civil lasers, rendezvous satellites, and space debris removal satellites can all be flipped quickly to perform anti-satellite missions. Those most eager to maintain America's advantage in space understand that excessive levels of secrecy must be relaxed if America's military, space industry, and allies are to work together effectively to stay ahead.

Excessive levels of secrecy must also be relaxed if America and its allies are to get ahead in advanced computational science, secure communications technologies, cyber and crypto techniques, and biological and health sciences—all key ingredients to winning next-generation conflicts and cracking open information fire walls (such as the Iron and Bamboo Curtains). In all this, the aim must be to increase the rate of innovation and to shorten acquisition times. This can best be achieved by expanding the number of qualified innovators and the ways they might safely collaborate, which, in turn, requires less not more secrecy while making the means to communicate protected information more readily available. To assure this, Congress must step up its game in overseeing America's classification and clearance system.

Might relaxing current clearance and classification levels risk more “leaks?” Perhaps, but using excessive secrecy to “protect” existing technology, which is about to become obsolete, will do far less to confound our adversaries than increasing our rates of innovation and acquisition. Improving these latter rates increases the number of projects and research efforts our adversaries must track and assess. Given that the ratio of success to failure is as often as one is to ten, easing classification should greatly complicate our adversaries' ability to “crack” what our next strategic technical advances might be, while prompting our enemies to spend valuable resources on time-consuming, expensive defensive measures.

Viewed in this context, America's penchant for relying on excessive secrecy to maintain its national security should no longer be viewed as a fix but rather as a problem. Hence, the need to clarify the national security dangers of excessive secrecy and to identify ways to reform our classification and clearance systems for the creation of an expert working group on classification and clearance policy reform.

In April 2020, the Nonproliferation Policy Education Center (NPEC) convened a discussion among national security professionals (current and former) to discuss the need for classification (and security clearance) policy reform. What began as an intellectual exercise to understand the true magnitude of the problem turned into a series of 12 workshops spanning a period of nearly two years.

The kick-off meeting was precipitated by a growing number of developments at the time that raised concerns over how the U.S. government's classification policies are impacting its national security. The Pentagon had just announced that it might be forced to classify the number of troops infected with the coronavirus as those numbers were reportedly spiking upwards. General John “Jay” Raymond, head of the U.S. Space Force, revealed that Russia had launched a spacecraft that was shadowing an important U.S. military satellite. When asked, he could not identify the U.S. satellite because that information was deemed classified. Nonetheless, Time Magazine broadcasted this to be the KH 11 spy satellite. In addition, there was continued and growing frustration from historians, academics, and those in the national security space over the State Department's constant inability to publish its *Foreign Relations of*

*the United States* volumes of key national security documents due to egregious delays by the Defense Department over-classification reviews.

With each meeting, it became clear that the problem was more pervasive than thought and even more difficult to address, as it permeates across the whole of the U.S. government's national security infrastructure. Each meeting brought a new set of issues to light, and provoked even greater scrutiny and discussion. After the kick-off meeting, the working group met 11 more times. Below is the schedule of meetings (with each meeting garnering a participation list of between 20-50 participants at any given time).

1. Kick-off meeting – April 23, 2020
2. Increasing Lack of Historical Documentation – May 27, 2020
3. Excessive Secrecy and Cybersecurity – June 24, 2020
4. Space Secrecy – August 10, 2020
5. Keeping Atoms for Peace from Being Overshadowed by Excessive Secrecy – October 28, 2020
6. National Security and Secrecy – December 2, 2020
7. Security Clearances: Barriers to Entry and Innovation – January 21, 2021
8. Are Australia's Classification Reforms a Model to Follow? – February 12, 2021
9. ITAR: A Security Clearance Barrier to Military Innovation – March 16, 2021
10. How Advanced Technology Can Dig America Out of Its Classification Jam – April 28, 2021
11. How the National Geospatial-Intelligence Agency Controls Its Secrets: The Way Forward for Our Government? – September 23, 2021
12. How Should Congress Manage Staff Access to Secrets? – January 26, 2022

What follows are brief reviews of each of these meetings along with the presentations that were given.

.

# Kick-off Meeting

## Working Group Series Meeting #1

April 23, 2020

**Background:** This meeting was scheduled in response to a growing number of developments at the time that raised concerns over how the U.S. government's classification policies are impacting its national security. The events specifically cited by NPEC were:

- the Pentagon had announced that it might be forced to classify the number of troops infected with the coronavirus as those numbers were reportedly spiking upwards.
- in February 2020, General John “Jay” Raymond, head of the U.S. Space Force, revealed that Russia had launched a spacecraft that was shadowing an important U.S. military satellite. When asked, he could not identify the U.S. satellite. That information was classified. Nonetheless, *Time* magazine broadcasted this to be the KH 11 spy satellite.
- the State Department's constant inability to publish its *Foreign Relations of the United States* volumes of key national security documents due to egregious delays by the Defense Department over-classification reviews.

The meeting featured brief presentations that delved deeper into these and other developments to examine how current security classification policies are impacting America's national security regarding: Historical analyses needed to improve strategic planning; speedy acquisition; allied information sharing; and the clearance of high-tech personnel in the fields of information technology, cybersecurity, aerospace, biotechnology, health sciences, and public health.

**Overview:** The working group began discussing the benefit received from the declassifying of historical documents, framed around the work done by David Rosenberg on the declassification of previously inaccessible documents used to help “change our understanding of nuclear planning.” Henry mentions a meeting in which Rosenberg stated he does classified histories for special access programs (SAPs) so that those running the SAPs can learn from the mistakes or successes of previous program managers running other similar SAPs. Apparently, David has said that because DoD has fallen so far behind in doing routine reviews, it was also falling behind in filing away classified documents. This led to a situation in which Rosenberg could not do his classified histories because he could not find the documents he needed.

“Information isn't any good if you don't use it.” The working group then began a discussion on space and the over-classification of space affairs. The speaker cites Space Force Commander

General Raymond as saying that there is a lot of activity by the Russians and the Chinese that we need to make the public aware of. He then moves into an anecdote about how over-classification can make things difficult. He pointed to his role in the Strategic Defense Initiative (SDI) and in the nuclear discussions with the Soviets. He said it was decided that the leverage the U.S. had with the missile defense program was in its competitive advantage, so it was decided to brief the Soviets on what the U.S. was doing in the SDI program. He said it took a year and a half to get the material declassified, but most of what they wanted to use was not releasable. But the briefing still had an extraordinary impact on the Soviets. One member notes that given what is going on in space, it requires an open discussion, particularly with friends and allies to convince them that these are things we need to pay attention to.

# Increasing Lack of Historical Documentation

## Working Group Series Meeting #2

May 27, 2020

**Background:** In the NPEC working group's kick-off meeting, William Inboden noted that sound strategic planning demands access to complete, documented, and relevant history. The group discussed the problem with timely access to documents and the roadblocks in the declassification process that has made gaining access to the relevant historical documents difficult. It was decided to make the increasing lack of historical documentation the focus of the second meeting of the working group. Ahead of the group's discussion, working group members prepared a brief memo for discussion. The working group was also provided the most recent Report of the Advisory Committee on Historical Diplomatic Documentation ahead of the meeting.

**Overview:** From the front end of the document and program creation process, to the middle leg of information sharing, to the back end of declassification...the United States government's national security departments and agencies are too quick to overclassify and too slow to declassify. Mr. Inboden's memo and the Report of the Advisory Committee on Historical Diplomatic Documentation points to the consequences: over-classification stifles information sharing, limits coordination across departments and agencies, restricts collaboration with allied governments and outside experts, and hinders oversight and accountability. In addition, the authors note that declassification backlog undermines transparency and accountability, fuels conspiracies, hinders problem-solving, erodes public trust in government, and threatens our national security.

The authors identify the following criteria for an effective (and efficient) declassification regime: preserving classification where needed, specified timelines that align with the goals of access and accountability to the public, and resources (people, funding, technology) that can sustain it. The authors then provide specific congressional initiatives to begin to mitigate the declassification "tail" of the problem, and they fall under the rubric of "Three Rs: Requirements, Resources, and Reporting."

**Needed New Rules:** The presenters made four recommendations:

1. Mandate all outside studies contracted by the Pentagon or the Intelligence Community be declared unclassified, "unless determined within 90 days of completion to take place at the classified level, or affirmatively found to contain classified information."

2. Amend P.L. 102-138 to specify that documents selected by the State Department Office of the Historian for declassification review and *Foreign Relations of the United States* inclusion (which are currently required to undergo interagency review within 120 days) shall automatically become declassified after a period of three years, absent affirmative reclassification by the originating department or agency **and** notification of Congress.
3. Require the CIA and the Pentagon to institute a 25-year mandatory declassification review of all documents, thus codifying in law this specific requirement under EO 13526.
4. Provide a congressional charter for the Interagency Security Classification Appeals Panel (ISCAP) and mandate that all decisions become precedents, binding on future document declassification reviews.

**Resources:** When documents started to go digital in the 1990s, the number of documents increased exponentially. These documents will soon be coming up for review. There is already a sizeable backlog and that pile will increase exponentially. Going through the backlog requires money, people and technology. The authors offer three recommendations for legislative action:

1. Mandate and fund development of artificial intelligence (AI) programs to expedite declassification. The Pentagon should do this through the National Defense Authorization Act, and the Director of National Intelligence through the Intelligence Authorization Act to incentivize competing approaches. Studies should include exploration of legal community's use of AI to review large volumes of information during discovery process.
2. Increase the National Archives and Records Administration annual budget by \$50 million and increase number of full-time equivalent workers designated for declassification review.
3. Mandate and fund training for U.S. government staff engaged in declassification efforts; training curriculum is to be developed and overseen by a National Declassification Center.

**Reporting:** The authors recognize the executive branch believes there are too many reporting requirements. Nonetheless, there is a need for oversight and advising. The Defense Department is particularly negligent, according to the authors. They provide five recommendations for legislative measures:

1. Charter the Director of National Intelligence as "Executive Agent" with authority to review declassification progress across the interagency (as per PIDB's recommendation).



2. Increase the authority of the PIDB to play a more active role in reviewing classification standards and processes and resolving declassification disputes and backlogs.
3. Create and (re) charter the CIA Historical Review Panel and a DoD Historical Review Panel (both modeled on the State HAC).
4. Require the Pentagon to submit a report to Congress every year detailing its progress on meeting its FRUS declassification obligations, and its plans to remedy any deficiencies.
5. Create a "Declassification Coordination" office in DoD headed by a Senior Executive Service official reporting directly to the Pentagon's Under Secretary for Policy with a statutory mandate to create a declassification coordination team to meet its declassification requirements and FRUS obligations.

The authors closed with this final suggestion: Each of the national security committees should have professional staff member positions whose responsibilities include declassification oversight. The national security committees so defined are: armed services committees of the House and Senate; intelligence committees of the House and Senate; the Foreign Relations Committee of the Senate and the Foreign Affairs Committee of the House; the Oversight and Government Reform Committee of the House and the Homeland Security and Government Reform Committee of the Senate; and the appropriations committees of the House and Senate.

In addition, the HAC worked with staff on the U.S. House Armed Services Committee to include a section in the National Defense Authorization Act of 2019 (NDAA) aimed at promoting DoD compliance with the Foreign Relations Statute. The provision requires the Secretary of Defense to submit a report to Congress on the "progress and objectives of the Secretary with respect to the release of documents for publication in the *Foreign Relations of the United States* series or to facilitate the public accessibility of such documents at the National Archives, presidential libraries, or both." This report should make more transparent DoD's performance and the reasons for its declassification delays, an important step in precipitating improvements.

The HAC urges DoD to take its cue from the CIA, notwithstanding the challenges that agency confronts in declassifying documents and meeting the mandated timelines for FRUS reviews. In fact, CIA's suspension in 2016 of the High Level Panel (HLP) mechanism that plays a vital role in evaluating OH's requests to acknowledge covert actions has contributed to the drop in the rate of FRUS publications, and OH still awaits 9 overdue responses from CIA on documents that OH submitted for declassification review. Still, CIA had resumed its participation in the HLP Ambassadors Daniel B. Smith (Ph.D. in History) and Julieta Valls Noyes, FSI's Director and Deputy Director, respectively.

As a result, direct discussions regarding resolving the issues have begun between the State and Defense Departments. The HAC strongly believes that integral to a viable resolution must be DoD's establishment of a process, and in 2019 it approved the first HLP issue since 2016. It also provided final responses on five volumes OH referred to it in previous years. Further, the CIA's declassification reviews and its responses to OH appeals are of the highest quality. This performance is a direct consequence of the dedicated FRUS coordination team that the CIA has in place. DoD should follow its lead.

### **The Review, Transfer, and Processing of Department of State Records:**

The HAC monitored the review and transfer of State Department records and their accession and processing at NARA.

Consistent with past several years, the Systematic Review Program of the State Department's Office of Information Programs and Services (IPS) made excellent progress in meeting its systematic declassification review requirements, responding to FOIA and MDR requests, and reducing its backlogs of both. Similarly, a new director appointed at the National Archives' National Declassification Center (NDC) reinvigorated the center's promotion of interagency cooperation, resulting again in reducing its FOIA backlog and processing hundreds of thousands of pages with a withholding-from-declassification rate of less than 10%.

What is more, signaling both tangible and symbolic progress, a joint venture by both State's IPS and NARA, led by the NDC, portends the resolution of problem that has festered for years. The two offices have formulated a yet-to-be-finalized plan by which IPS will perform the initial declassification review of the 1981 and 1982 N and P reels (microfilm of previously destroyed documents), perhaps at the secure NDC site. If implemented, this strategy will overcome the security and technological obstacles that have brought these reviews to a standstill.

The HAC compliments IPS and NARA on this initiative and will monitor progress toward bringing it to fruition. Yet it is concerned with other potential problems that loom ahead, all of which the HAC raised in the 2018 report and have if anything become more acute. These include budget-driven reductions in NARA's personnel that slowed the accessioning and processing of State Department records and adversely affected researchers' experiences by, for example, normatively producing skeletal finding guides rather than the detailed ones that researchers require. A greater concern is the capacity of both NARA and the State Department to manage the explosion of electronic records.

Developments in 2019 all but assure that this management challenge will intensify. A memorandum issued jointly by NARA and the Office of Management and Budget in June directs all agencies to manage in their entirety their permanent records electronically by December 31, 2022. This directive demands that the agencies digitize all their remaining paper records because NARA will no longer accept paper records after that date.

This policy confronts each agency with an unfunded mandate that, in an era of constrained budgets, staff shortages, and an urgent need to purchase advanced technologies, imposes a cost that creates a severe burden on them. The HAC imagines a scenario in which departments and agencies hold their documents hostage and do not transfer them to NARA until they receive additional appropriations. In worst-case scenarios, the poor quality of the digitized records renders them unusable, or agencies even destroy records. The State Department anticipated the digital deluge, and according to IPS, “is currently developing plans to comply with the June 2019 OMB and NARA mandate for transitioning to electronic records.”

The HAC did not receive a briefing on those plans. (The HAC chair and another member received abbreviated briefings.) In December, however, the IPS director distributed to the HAC a paper on its modernization program. It made explicit that IPS applauded NARA’s establishing benchmarks for achieving a fully-digitized records management system and enthusiastically embraced the challenge of meeting those benchmarks. The HAC understands that enthusiasm for modernizing records keeping. Yet it is concerned that the IPS paper neglects to discuss the costs of the modernization program and the potential risks that inhere in such a rapid transition from paper to electronic records management.

The paper focused on the development of new records disposition schedules, a core concern of the HAC. IPS has pledged to present full briefings in 2020. The HAC intends to use these briefings to raise fundamental questions about the costs and risks. It anticipates asking: 1) How the consolidation of records into “big bucket” schedules will affect their discoverability by researchers? 2) What is the likelihood that in the rush to transition to big bucket records schedules valuable records will be mistakenly categorized as temporary and thus earmarked for destruction? and 3) Is it realistic to expect IPS to complete the modernization program in two years, and what if it does not?

The HAC also worries about the effects of budgetary and staff shortages on the Presidential Library system. NARA is transferring to the NDC all classified records held at the libraries, anticipating an expedited declassification review. The processing and classification review of emails from the Reagan and George H.W. Bush administrations continue to be stalled for lack of resources. Solving these problems is central to the future research needs of FRUS compilers and the public at large.

### **Recommendations:**

- Senior State Department Officials should work with counterparts at DoD to establish a centralized FRUS declassification coordination team which can more effectively meet DoD’s mandate for the timely review and release of historically significant information that no longer needs to remain classified.

- NARA and IPS should solicit public comment on plans to convert to technologically-driven records management and big bucket records disposition schedules.

Minutes for the HAC meetings are at <https://history.state.gov/about/hac/meeting-notes>.

---

## **The Classification Crisis, from Tooth to Tail**

### **Meeting Memo from William Inboden**

Amidst our nation's many other challenges, some quite severe, the United States has a classification problem. The corollary is also true: the United States has a declassification problem. From the front end of the document and program creation process, to the middle leg of information sharing, to the back end of declassification – or from tooth to tail, to borrow a phrase – the United States government's national security departments and agencies are too quick to overclassify and too slow to declassify.

This tangle of classification pathologies brings many harmful consequences. Overclassification stifles information sharing, limits coordination across departments and agencies, restricts collaboration with allied governments and outside experts, and hinders oversight and accountability. The nebulous realm of studies conducted by outside consultants stuck in "classification limbo" (neither determined to be unclassified or classified, with no timeline for resolution, and thus subject to absurd restrictions on use and dissemination) chokes independent expertise and partnerships. The declassification backlog undermines transparency and accountability, fuels conspiracism, hinders problem-solving, erodes public trust in government, and threatens our national security.

The good news is that reforms to these areas, including a credible and efficient program of declassification, would bring many benefits. To take one example, the documentary declassification successes of the past few decades bear witness to this. In the words of Bill Burr of the National Security Archive, "declassification is vital to a thriving democracy. Not only does it help the public hold leaders accountable; it also allows for a more accurate and comprehensive accounting of the past."<sup>1</sup> Senator Ben Sasse highlighted another advantage in his September 6, 2019 letter to the NDAA Conferees: "National security scholars and professionals rely heavily on declassified policy documents of past successes and failures to inform their work and analysis. Research informed by primary documents organically leads to more accurate and effective policy advice to current policymakers."

An effective declassification regime should follow these criteria: (1) preserving classification where needed, (2) specified timelines that align with the goals of access and accountability to the public, and (3) resources (people, funding, technology) that can sustain it.

These problems span generations and will not be solved by a three-page memo. But this memo does suggest some specific congressional initiatives that, taken in part or in whole, would help begin to mitigate the declassification “tail” of the problem in particular. These suggestions fall under the rubric of the “Three R’s”: Requirements, Resources, and Reporting, William Burr, “Trapped in the Archives,” *Foreign Affairs*, November 29 2019.

### **A) Requirements**

This refers to the thicket of laws, executive orders, department standards, and other mandates governing the classification and declassification process. Effective information sharing and efficient declassification starts with requiring that it be done. Suggested legislative measures:

- 1) Mandate that all studies contracted by the Department of Defense and/or Intelligence Community to be conducted by outside consultants (such as RAND) be declared “unclassified,” unless determined within 90 days of study completion to take place at the classified level, or affirmatively found to contain classified information.
- 2) Amend Public Law 102-138 to specify that documents selected by the State Department Office of the Historian for declassification review and FRUS inclusion (which are currently required to undergo interagency review within 120 days) shall automatically become declassified after a period of three years, absent affirmative reclassification by the originating department or agency and notification of Congress.
- 3) Require the Central Intelligence Agency and Department of Defense to institute 25-year mandatory declassification review of all documents, thus codifying in law the requirements of E.O. 13526
- 4) Provide a congressional charter for the Interagency Security Classification Appeals Panel (ISCAP) and mandate that all ISCAP decisions become precedents, binding on future document declassification reviews.

### **B) Resources**

The mountain of documents awaiting declassification review, already daunting, is about to erupt into a cascade of digital information overload as the U.S. Government’s transition to

electronic documents that began in the 1990s begins to bump up against declassification mandates. Working through the growing backlog and looming deluge of documents in need of declassification review takes money, people, and – especially – technology. Suggested legislative measures:

- 1) Mandate and fund the development of Artificial Intelligence programs to expedite declassification (CIA has launched a promising pilot project but seems stalled for lack of support). Suggest requiring DoD to do this through NDAA and DNI to do it through IAA to incentivize competing approaches. Studies should include exploration of legal community's use of AI to review large volumes of information during discovery processes
- 2) Increase NARA's annual budget by \$50 million and increase number of FTEs designated for declassification review
- 3) Mandate and fund training for USG staff engaged in declassification efforts; training curriculum to be developed and overseen by National Declassification Center

### **C) Reporting**

While the executive branch already groans under burdensome reporting requirements, the mantra “that which does not get measured does not get done” remains true. The following measures take a broad view of “reporting” to include oversight and advising; the reporting requirements are designed to be succinct and targeted. The Department of Defense gets singled out because it is singularly negligent. Suggested legislative measures:

- 1) Charter the DNI as “Executive Agent” with authority to review declassification progress across the interagency (as per PIDB's recommendation)
- 2) Increase the authority of the Public Interest Declassification Board (PIDB) to play a more active role in reviewing classification standards and processes, and resolving declassification disputes and backlogs
- 3) Create and (re) charter the CIA Historical Review Panel and a Department of Defense Historical Review Panel (both modeled on the State HAC)
- 4) Require the Department of Defense to submit a report to Congress every year detailing its progress on meeting its FRUS declassification obligations, and its plans to remedy any deficiencies

5) Create a “Declassification Coordination” office in the Department of Defense headed by an SES reporting directly to the Under Secretary of Defense for Policy, with a statutory mandate to create a declassification coordination team in order to meet its declassification requirements and FRUS obligations

A final suggestion for Congress: Each of the national security committees ought to create/designate a PSM position whose responsibilities include declassification oversight. This includes the Senate and House Armed Services Committees, Senate and House Intelligence Committees, Senate Foreign Relations and House Foreign Affairs Committees, House Oversight and Government Reform Committee; Senate Homeland Security and Government Reform Committee, and Senate and House Appropriations Committees (or appropriate subcommittees).

# Excessive Secrecy and Cybersecurity

## Working Group Series Meeting #3

June 24, 2020

Harvey Rishikof with the American Bar Association Standing Committee on Law and National Security gave a presentation to the NPEC working group on how excessive secrecy harms the cause of cybersecurity. This working group's session had 33 attendees comprised of early, mid-career, and senior officers; and staff from the military, Pentagon, Intelligence Community, Department of State, Government Accountability Office, National Archives, Records Administration, the U.S. House of Representatives, and U.S. Senate. In addition, senior retired officials, outside government advisers, academics, legal scholars, and other policy experts contributed to the working group. Prior to the meeting, NPEC circulated to the working group a two-page read-ahead memo by Mr. Rishikof entitled "How Over-classification Undermines America's Cybersecurity," (See below).

The workshop discussion focused on "zero days" and the dilemma on how and when (or rather if) these vulnerabilities should be shared. The arguments fall on what responsibility, if any, the government has to share information on zero days and to improve the cyber ecosystem. Rishikof cited a Microsoft flaw that was discovered by the IC that was so structurally problematic that a decision was made to make it public so it could be corrected. However, he also sites examples from his time in the private sector when corporations and companies are reticent to come forward and inform the government of an attack on their networks for fear of being prosecuted for negligence and afoul of regulations.

Rishikof noted that he has been working on the issue of transparency and information sharing in the public-private world for cybersecurity for the past 30 years. He points to a report he worked on with MITRE called "Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War," which recommended an entity be created under the counter-intelligence directorate that would include the IC, DoD, DOJ, FBI, and DHS which would "gather the information and keep it classified where it had to be but also they'd be able to *pass the information back through to the companies when it was appropriate.*" He says they have not been able to solve this riddle.

In closing, Rishikof suggested that this entity should be housed at the National Counterintelligence and Security Center (NCSC) – and that there will need to be legislative relief (NDAA, IC Authorization) to create this entity. He also suggests the ability to grant immunity to certain companies so that they can feel comfortable sharing information. A need to "illuminate the supply chain."



## **Questions and Answers:**

- 1. Could you walk us through how the National Supply Chain Intelligence Center would operate? NCTC model? How would the information be shared?**

**A:** While skeptical of the NCTC model it really was a failure of leadership, the model could work if done right. This would bring together all the authorities in a manner similar to that of a joint task force, which would have all the authorities required, particularly with giving immunity to companies that have been attacked or have vulnerabilities but don't want to share out of fear of being held accountable.

With respect to the sharing of information, there are cleared individuals in the DIB. They should be given the information relevant to them (there is a vulnerability or flaw that needs to be addressed) without worrying about sources and methods (how you became aware of this).

- There was a DNI directive that replaced Need to Know with Responsibility to Provide – nobody knows it exists.

- 2. There is already a supply chain group at NCSC, so how is this different? Industry has been trying to get the sharing of personnel information in a post-Snowden environment, and it's actually been the NCSC Director saying it's not me, it's the lawyers, and the lawyers are saying it's not us, it's the policy, and the policy is saying it's not us, it's the policy.**

**A:** We need to gather the lawyers and get them all together and have them state, which statute, what law, what are you using as your justification for preventing the sharing of information.

- 3. E.O. that governs classification states that open government is a co-equal priority. New national intelligence strategy speaks to partnerships, which acknowledges there is a problem that needs to be solved.**

**A:** We need to let the private sector feel comfortable that it can share information. Blend the tools and authorities so that DoD can operate and track on DHS networks, DHS can do the same, and they so that they can also operate on DIB networks and see what they are seeing.

- 4. This is not U.S. only policy, but we work with allies – interoperability problems with allies? Also, you will never solve this problem through leadership or bureaucracy, only organizational structure.**

**A:** Security is not seen as a profit center; it is a cost center. Organizations now are looking to save costs – they are only looking for good enough. This is not sufficient. Security needs to be a discriminator for purchase. How do we make security a “coolness factor” for businesses that would make them want to prioritize security over other factors. Do you incentivize them with tax credits?

- 5. Transparency – seems you are talking about some form of internal transparency that may actually involve greater secrecy with respect to the public. Contractors provide information to DoD with the caveat that it guarantees it doesn't become public. We may even need a new FOIA exemption to guarantee it doesn't become public. So, am I correct that in order to reduce internal barriers to information sharing, do you think it may also be necessary to increase barriers with respect to public disclosure? And do you see a role for greater public disclosure in this area?**

**A:** What is FOIA-able? Will we need a new exemption? Only DHS currently has the power to provide immunity under the current framework. DIB and others need to know they will not be held liable.

- 6. What exactly do individuals and entities need to know and how do you craft the information they need and don't get? If we provide people only with the what they need to know, but not how you got that information, why will people trust you that they will be acting on good information? Government needs to say no to low bids if they believe they are not transparent enough and they don't have faith in their security/supply chain. Scandals will get people's attention, particularly Congress', in order to get them to act on this.**

**A:** On being told something is wrong – you would take it at face value if being told from one of your own people. The cleared individuals or the CEO may be aware of the full picture and can instruct accordingly.

- 7. If you were going to ask for 3 specific legislative and executive actions on this, what would they be?**

**A:** First, need to have a center for the supply chain under DNI to have extraordinary authorities to share information both ways with a level of immunity. Second, the NDAA for 2018 had a range of projects (Section 1696), but they never funded it. Third, asking for a classified hearing for DoD, IC, DHS and FBI and ask them to explain what is actually their cyber framework for understanding what the vulnerabilities are and then crafting a strategy to go offensive in persistent engagement.

## **How Over-classification Undermines America's Cybersecurity**

### **Meeting Memo from Harvey Rishikof**

I would say this over-classification issue in cyberspace, or the classification in general, is an issue we have been fighting concerning the number of attacks and the sharing of information between the public sector and the private sector. We have clearly not resolved the issue of the public private sharing of information in the context of the cyberthreats. I would say that when I was on the government side in counterintelligence there were certain types of information we had that I think the private sector would have liked to have had but we had a number of restrictions either with legal frameworks involving violations of antitrust or a decision on the government side for sources and methods. We did not want to give up the information because of the fear of burning the asset. And we did not have a systematic, I would say, policy approach for how we racked and stacked the assets and which assets might have been worth us sharing the information so that it would have improved the ecosystem of the cyber world.

We have a similar problem with the issue of how we dealt with the concept of zero days. Those are, as you know, flaws in a code that have never been seen but that are discovered by individuals reviewing the code which allows us access to exploit those zero day codes in order to make a penetration or to cause a cyber effect. The attack on the nuclear facility in Iran as an open source proposition had at least three zero days that were involved in that operation that were exploited [by] whoever was the aggressor to get into that facility. So that issue of what is the appropriate balance of sharing information on the government side when it has these types of zero days and what it should be doing to improve the ecosystem, again, has not produced a consistent and structural policy.

We recently had a moment in which the intelligence community came forward with a fix for a Microsoft problem. The decision was made that the problem was so structural in the Microsoft app, the platform, that it should be made public in order for it to be fixed. On the other side, when I wear my private sector hat, there is a deep resistance in major corporations and companies to be able to come clean with attacks that have taken place on their networks and their willingness to share with the government for fear of either being prosecuted because it would demonstrate that they had been negligent or potentially grossly negligent in some aspect of their network maintenance. There is fear that if they share the information that information will be shared with the inappropriate regulatory group and that regulatory group would then penalize them for their inaction on the network. So that level of the need of transparency in the public private world, in the sharing of information given our vulnerabilities in cyber, is something that literally I've been working on or involved with, it's embarrassing to say, for almost over 25 years, 25 or 30 years. And it's a very similar conversation that happens all the

time; and we in a report that I was involved with at MITRE called “Deliver Uncompromise,” we recommended that there be an entity created, probably under the counter-intelligence directorate that’s under Bill Evanina. They should be able to have jurisdiction that would include both the intelligence community, the Department of Defense, DOJ, the FBI and also the DHS. All of the authorities under one hat so that they could gather the information and keep it classified where it had to be but also they’d be able to pass the information back through to the companies when it was appropriate. We have not solved that riddle.

Now going forward, there are some people on the call, trying to get that piece of legislation and that put in the bills for either the NDAA or else with the IC Authorization Act in order for the U.S. to create this entity. It's similar to the entity that we created for the National Counterterrorism Center (NCTC). The NCTC has had some degree of success in sharing information and gathering information. And I think we clearly need something in the cyber arena that is similar.

Alex has just pointed out I was referring to the National Counterintelligence and Security Center. The NCSC is where we thought it should be housed. We got a little bit forward in the last IC and NDA but not all the way there. But this is a huge problem that I think requires some legislative response in order for us to be able to grant immunity to certain companies so that they can feel comfortable sharing that information. We need to “illuminate the supply chain” in order to move forward to be more securing of the post 9/11 world where our adversaries are using asymmetric cyber vulnerabilities.

# Space Secrecy

## Working Group Series Meeting #4

August 10, 2020

**Background:** For its fourth meeting in national security classification and clearance policy reform series, the working group met to discuss classification issues surrounding space secrecy. In preparation for the meeting, NPEC circulated two articles: “Stovepipes in Space: How the U.S. can overcome bureaucracy to improve capabilities” by Dennis Blair and Robert Work, and “Nominee to lead Space Command voices support for declassifying space” by Nathan Strout.

In Stovepipes, the authors argue the over-classification and compartmentation of both program and intelligence space information are making for a less efficient and less effective effort in standing up the Space Force. In order to overcome this impediment, they argue, it will require a personal push from the entire leadership of DoD and the IC. Undoing the “norm” set in the early days of the space race of compartmentalizing and classifying space programs at the highest levels takes a sustained effort. They argue that the “partitioned nature of space program classification still remains and far exceeds that of other equally sensitive domains— air, land, sea, undersea and cyber.”

The authors then identify three harmful effects impacting the current system: duplication with space acquisition programs; nonexistent or rudimentary integration of space capabilities into the plans and exercises of combatant commanders; and, ignorance of specific space threats.

On the first, they argue that within the multilayered security compartmentation in the space domain, there are duplicative efforts undertaken to solve the same problems, but others are unaware (even within the same organization). This results in wasted resources and missed opportunities.

On the second, they argue that space programmers brief their combatant commander and are then told they cannot talk to anyone else about the program, lest they face prosecution. But the four-star is unable to fold the capability into the operations plan of the command, and without knowledgeable operations staffs to exercise the programs, they will not be effective when it comes time to implement them.

And finally, on the third point, they argue that despite Russia and China deploying space-based systems that threaten forward-deployed American joint task forces at sea, in the air, and on the ground, these threats are so highly classified that the deploying forces are unaware of them. Currently, information like this can only be provided to forward forces with extraordinary

precautions that make it late and often useless. And the situation is even worse when it comes to sharing relevant information with allied forces.

Despite identifying the problem, the authors offer little in the way of recommendations to reform the situation. They point to powerful bureaucratic forces invested in the current system and note that the rewards for sharing information are far less than the penalties would be of mishandling highly classified space information. They say it is almost impossible for a military commander or civilian official to overrule the security bureaucracy.

They do, however, offer one recommendation: establish a high-level commission of former officers and officials to recommend a better system. The commission should be charged to document the costs of the current system, then to come up with a better one that will protect information to a high degree while allowing much greater sharing across acquisition programs, between programs and operational forces, and between the intelligence community and operational forces.

**Read-ahead Background Memo:** In preparation for the discussion with the working group, Brig. Gen. (ret) S. Pete Worden prepared a memo further discussing the issue. He states that “civilians in DoD have pushed back against reasonable requests to reform our security clearance policies.” He goes on to identify two classes of problems excessive secrecy is producing: harm to timely hiring, contracting, acquisition, information sharing with contractors, allies, and to the public for essential public policy and diplomacy. He argues this requires reducing the level of classification. The second is that the special access programs (SAPs) are so compartmentalized that only the most senior officials know about them. This results in likely duplication of efforts and being unaware of solutions or improvements that could help in planning or programming. He argues that Congress may need to hear of horror stories in the conducting of its oversight to spur real action on reform. However, this may be risky to national security and peoples’ careers and contracts. He then states that Blair and Work’s suggestion of a commission is insufficient.

Instead, he poses two suggestions: pass a law noting the complaints he has highlighted and require the National Space Defense Center to create a hotline that would take anonymous tips (specific case complaints) and how excessive secrecy is harming timely hiring, contracting, acquisition and information sharing. These are investigated and anything valid is provided to Congress (he specifically states HASC and SASC) in a classified and unclassified report after two years.

The second suggestion is to add a requirement that the Joint Space Operations Center submit a classified report annually for two years detailing in what areas excessive secrecy or failure to follow required coordination methods resulted in programs costing more and being less mission effective. The report could include remedies the Center thought might promote better communication and more efficient programs while protecting sensitive programs.

**Meeting Discussion:** Henry opened the working group meeting by noting that Senator Rounds had been presented with the Blair/Work op-ed as well as the read-ahead memo and requested a meeting with General Dickinson (at the time, nominee to be Commander, USSPACECOM, is now the current Commander). This resulted in a back and forth between the nominee and the Senator at the General Dickinson's nomination hearing<sup>1</sup> in which they discussed the problems with excessive secrecy. Senator Rounds indicated he would like to hold a hearing on this issue. Henry also noted the SSCI indicated they were going to hold a hearing on this issue – both open and closed. This did occur., though it was broader than just space related.<sup>2</sup>

Lt. General Worden then discussed his memo. He reiterated that stovepiping to this extent makes it hard to get the best and brightest into these fields important to national security. If young people don't understand why this is important to our country and our country's security, it's hard to get them to the right career paths. He also raised the significant issue of working with friends and allies around the world – “if you can't explain why there's a serious threat and you can't explain what it is you are actually doing, it's hard to get contributions.” He noted a similar problem with the commercial sector. Finally, he notes that because of the excessive secrecy, there is no professional/public review of a particular program (from his experience particularly with space, though this is likely true throughout the USG), which leads to mistakes being made that go uncorrected yet hundreds of millions of dollars get wasted in continuing with the project/program.

Henry raises that he had discussions with Hill aides who stated that it would be important to hear these stories. Which Henry then noted, was unlikely to happen because of the over-classification and excessive secrecy – nobody will have the clearance to hear the stories and nobody can share them publicly, so it's stuck in this loop. Henry suggests that instead of legislating a solution, perhaps we need to figure out whether we can get more stories and how? It was argued that it had to be filtered. Other ideas were shot down. One suggestion that survived was: you could designate an organization in the executive branch to act as a receiver/reviewer of anonymous phone calls within the system complaining about something.

One participant noted that this is a small problem that is part of the larger problem of over-classification. The system is based on outdated operations and guidelines. There are appeals processes that are supposed to be in place that are not used as often as they should be. Henry notes that while all that is true, the focus here is to point to the cost or dysfunction created by the problem of declassification.

It was then suggested to use historical examples that exemplify the issues. Henry reiterated that the congressional aides noted that they “need something that, if not on fire, has smoke coming

---

1. [https://www.armed-services.senate.gov/hearings/20-07-28-nominations\\_vanherck--dickinson](https://www.armed-services.senate.gov/hearings/20-07-28-nominations_vanherck--dickinson)

2. <https://www.intelligence.senate.gov/hearings/open-hearing-declassification-policy-and-prospects-reform> for the open hearing; there is no indication when or if this was done in a closed session.

out of it.” Another member of the working group raised a point that what is missing from the discussion is a sense of the standards of when secrecy excessive. He believes that no amount of stories – however horrendous they might be – are going to tip the balance unless you can also get a sense of what the counter-argument is. There was then a back and forth on this, with some arguing that the argument in need of reform cannot be that it blocks the flow of information and is inefficient, because that is precisely why things are kept secret – to block the flow of information. Others argue that is the point – we shouldn’t be discussing it in generalities, but by giving it a name and a face with concrete examples, we can start the much needed argument.

They then discussed the difficulty in finding the right balance between transparency and the real need for secrecy. It was suggested that first a model needs to be constructed on how to handle classification and what should be shared. It was also noted that the penalties for revealing classified information, intentionally or not, greatly outweigh those for over classifying information – at least on the personal level.

Another workshop participant then circled back on the idea of having a body whose mission already includes looking across compartmented programs and making sure compartments talk to each other and do what they are supposed to do. He states there are some that do this already and work well. But he supports the idea of having these bodies report to the Hill, in a classified report if necessary, or to the Gang of Eight if so highly classified.

It was then argued that this issue needs to be looked at in the general, bigger picture sense because it cannot be chipped away at piecemeal. In the broadest sense, we are dealing with three interconnected issues: how things are classified, how they are protected, and how they are declassified. And this is true across the board and not just of space policy. So, if you try to chip away at the problem – a specific problem – without trying to address the more broad and overarching problem, you will not be able to make any progress. This problem is so enduring, so systemic, so deeply rooted, that we haven’t made any significant changes over the years to accommodate the extraordinary problem of proliferation of classified information (over and under classification). The question of how to tackle this again was raised. One suggestion was the trick is engaging both the executive and Congress. It was pointed out that this is what this exercise is for.

The question was raised as to how the NSA is, in theory, able to manage secrecy with protecting its programs and mission, to which the response was that NSA differs from the space programs because there isn’t a big commercial aspect to what NSA does nor is there a commercial equivalent to the NSA. Space also has a much bigger public excitement and global interest – it is inherently a global public area. It was then suggested to make a list of what are the criteria that something needs to be highly classified and stay that way for a long period of time and then ask why is space not like that now and what parts of space need to stay that way.



It was then pointed out that, rather than looking at the NSA model, attention should be paid to the NGA model. NGA is looking at some parts that are quite highly classified, figuring out how to downgrade them, and then get them out to their customers in a wide and quick range. They are bringing in people for the innovation factor because it is cool to work on this stuff. They have a new classification guidance that is updated monthly and in real-time. This idea was supported and then it was suggested that there are also things the NSA did, pointing to creating the Gamma channel and then clearly identifying people who need to know that information. A similar thing could be done for space – create a space specific channel that everyone who needs to know could use and access. This could allow information to be moved from SAPs to a controlled channel.

A working group member took issue with using NSA as a positive example of anything, stating it is the agency that is the most difficult in terms of information sharing not only across other agencies, but within the agency itself. But this member did endorse the NGA model. They then asked: Strategically where are we going? If we focus on space, will there be a trickle-down effect – any progress we make in one area, will it make it down to the benefit of the larger questions across the entire series? Henry responds: This area has been shot at by lots of folks – lots has been done. But the government has been resilient to what we would like it to do – be more transparent. The executive doesn't have incentives to do that (though NGA makes sense because there is a civil and military customer and space is similar). More generally, Congress has not been as engaged as it could be (staffers don't have the needed clearances to play the oversight game) and because the members don't particularly care and stay hands off unless they have specific concerns. The thought is if there are enough stories, enough problems, enough op-eds about operational problems for National Security writ large, you might get Congress more engaged so that, at a minimum, you might get staffers engaged and interested in certain parts of the problem, though recognizing there is a larger problem, and may focus efforts toward fixing the problem. It was also noted that the stories shared with the Hill can't just be horror stories of how bad things are, but also show examples of where the sharing of information produced a positive effect.

It was then raised that one layer of the bureaucracy that is difficult to engage but worthwhile if you can do it are the Inspectors General. It was noted that all IG reports go to Congress and are of interest to Congress, and that all Inspector General (IG) offices include an auditing section. Henry asks if Congress has any authority to contact the IG – it was questioned and not definitively answered. One commenter noted that Congress can, but the IG doesn't have to listen. A Senate staffer chimed in that it was “most appropriate” for Congress to talk to IGs because the IG ultimately gets confirmed.

There was then a discussion on the Government Accountability Office (GAO) and the utility of using the GAO to get the ball rolling. It was noted that GAO was not an “end-state” but rather used to then generate legislative ideas that get converted into legislative language.

On closing, it was suggested that there might be a new executive order on this issue that a new administration might look into.

---

## **Discussion on Excessive Secrecy in Our National Security Space Programs**

### **Meeting Memo from Pete Worden**

**Problem:** General Raymond, former Secretary Wilson, General Hyten, Dennis Bair and Robert Work have all recently complained about how excessive secrecy is jeopardizing achieving America's military space objective. Blair and Work's most recent oped of two days ago (attached below) comes closest to identifying the problems excessive secrecy creates for our military space efforts but, to date, civilians in DOD have pushed back against reasonable requests to reform our security clearance policies. There are two classes of problems excessive secrecy is producing. The first class is harming timely hiring, contracting, acquisition, information sharing with contractors and allies, and the release of information for essential public policy and diplomacy. This class of problems requires reducing the level of classification (and, in some cases, totally declassifying information) to allow a wider sharing of information. The second class of problems is America's most sensitive special access programs relating to space are kept so secret and compartmentalized that only the most senior officials know about them. As a result, folks at the working level may not even be aware that their own planning and programs would be improved by the capabilities within a related compartmented program. There also is a risk of costly, unnecessary duplication of effort. With regard to both classes of problems, what Congress lacks and needs to accomplish its constitutional duty of oversight is to get specifics, i.e., actual horror stories. Finally, the lack of critical review inherent in highly classified, often compartmentalized programs can and does result in expensive failures and proceeding down unpromising paths. The telling of such tales, however, is risky to a. Our national security and b. Peoples' careers and contracts. Blair and Work recommend creating a commission. This may gain support but alone may prove to be insufficient. In any case it would take at least two years to produce any findings.

**Remedy:** Take two steps. To gain greater fidelity on the first class of problems excessive secrecy causes, pass a law noting the complaints above and require the National Space Defense Center to create a hotline that would take anonymous tips (i.e., specific case complaints) about how excessive secrecy is harming timely hiring, contracting, acquisition, information sharing with contractors and allies, and the release of information for essential public policy and diplomacy. The Center would be required to validate as many of the complaints as possible annually in both a classified and unclassified reports to the HASC and SASC for two years. This duration would allow Congress to learn if things are getting better, staying the same, or

getting worse. It also would give the HASC and SASC the grist to determine, what, if anything, might be done to improve matters. For the second class of problems created by excessive secrecy, add a requirement that the Joint Space Operations Center submit a classified report annually for two years detailing in what areas has excessive secrecy or failure to follow required coordination methods resulted in programs costing more and being less mission effective. This report would include whatever remedies the center thought might promote better communication and more efficient programs while protecting highly sensitive programs critical for U.S. national security and war fighting.

# Keeping Atoms for Peace from Being Overshadowed by Excessive Secrecy

## Working Group Series Meeting #5

October 28, 2020

**Background:** The NPEC working group invited Sharon Squassoni of George Washington University to brief on “Keeping Atoms for Peace from Being Overshadowed by Secrecy.” Ms. Squassoni was formerly with the Arms Control and Disarmament Agency (ACDA) as well as the Congressional Research Services (CRS). Posed to the group for discussion was the question: what can and should the U.S. government do to reverse the trends of increased opacity of U.S. nuclear export licensing, intangible nuclear technology transfers, nuclear cooperative agreement negotiations, and nuclear proliferation intelligence? Citing Saudi Arabia as the poster child for these problems, NPEC noted that there are other cases as well that should be of concern.

**Read-ahead Background Memo:** Ms. Squassoni’s memo, “Keeping Atoms for Peace from Being Overshadowed by Secrecy: The Case of Nuclear Exports” was distributed to the working group in preparation for the discussion. She provided a brief summary: “There is increasingly less transparency about nuclear cooperation agreements, export licensing, export controls and the value of exports from the U.S. nuclear industry. There is also less information made available to the public about nuclear proliferation trends. It will become increasingly difficult for policymakers and outside experts to connect the dots between what the U.S. is subsidizing, exporting, and how it is being used or misused by partners and competitors alike to reduce or exacerbate proliferation. The U.S. Congress and the next administration can make changes to return to or increase transparency and thereby vastly improve policymaking capabilities.”

She begins by noting that one area that defies the modern convention of instantaneous posting of sensitive information or inadvertent release of information is the nuclear power sector, which has become increasingly opaque. She notes that there is a desire by the U.S. government to promote nuclear exports at the expense of critical reviews, supported by the nuclear industry and the claim that it is essential to U.S. national security. In turn, this has resulted in the streamlining of export licenses and reviews of nuclear cooperation agreements.

She then lists eight reasons, as outlined in the 2020 Energy Department strategy to restore America’s nuclear competitive advantage, how U.S. national security is assured through nuclear energy:

1. Uranium is a critical mineral.

2. Importance of nuclear energy for resilient electricity/critical infrastructure.
3. DoD needs nuclear power for forward operating installations.
4. Dependence on global nonproliferation and safety, which U.S. champions.
5. Importance of foreign policy relationships (cemented by nuclear cooperation).
6. LEU for tritium production for nuclear weapons and HEU for naval reactors.
7. Assured uranium stockpiles.
8. Civilian workforce base.

She also lists the four objectives of the strategy: provide immediate financial support/subsidies to U.S. uranium mining and the front end of the fuel cycle; decrease permitting and regulatory burdens on industry in the front end; support advanced technology and empower U.S. export competitiveness.

She states that the major corresponding policy to these objectives resulted in “pushing nuclear cooperation to the sidelines of 123 agreements,” and had the following impacts: more secrecy about Part 810 authorizations, designed to protect firms rather than U.S. nonproliferation interests; more secrecy about 123 agreements and less information to Congress; and, more secrecy about nuclear exports and their value.

With respect to Part 810s, Ms. Squassoni argues that the Energy Department began faster processing of these authorizations, which meant looser restrictions around the export of nuclear technology assistance to countries with which the U.S. may not have a full nuclear cooperation agreement. She cites processing time for Part 810s in 2019 being cut in half, as reported to Congress in the annual report on Transfers of Civil Nuclear Technology. She also states that the report gave no actual specifics regarding kinds of technology or information, countries, or suppliers. She notes there is no requirement to inform Congress, but that DoE, within a month of granting a specific authorization, may provide a copy of that authorization “to any person requesting it at DoE’s Public Reading Room, unless the applicant submits information demonstrating that public disclosure will cause substantial harm to its competitive position.” She notes that DoE authorized eight Part 810s for Saudi Arabia, but unlike previous authorizations, these were kept secret to “protect proprietary information” at the companies’ request.

On Section 123 Agreements, Ms. Squassoni listed the following ways the executive branch has acted to minimize scrutiny of nuclear cooperation agreements: consultation only comes at the end of the negotiating process with a final copy of the signed agreement to approve sent to Congress; the nonproliferation assessments required by law have become pro forma, with some

failing to mention former nuclear weapons programs in partner countries; and, the adoption of rolling extension and unlimited duration treaties without any requirement for periodic review. She also noted that the text of previous 123 agreements has been removed from the DoE website. She then noted then-Assistant Secretary for ISN Chris Ford's push at the State Department for NCMOUs – Nuclear Cooperation Memoranda of Understanding – and states that it was unclear whether they were meant to supplant 123 Agreements or merely pave the way for easier negotiations.

Turning to the nuclear industry and its claims on the value of nuclear exports, jobs, and the economy, Ms. Squassoni questioned the industries assertions as compared to the Bureau of Labor Statistics data. The Nuclear Energy Institute claims that a single nuclear power plant generates more jobs than any other type of electricity generation station, claiming that each plant employs 500-1000 workers; construction peak requires 3500 workers; salaries are 20% higher than for other electricity generating plants; and that each plant creates \$40 million in labor income each year. With respect to exports, NEI estimated years ago that the nuclear export market could bring 185,000 U.S. jobs and \$125 billion in revenue for a 10-year period between 2014-2024. Citing a CRS report from 2014, fuel exports only accounted for \$1.9 billion while other nuclear technology constituted \$350 million.

She closed by making the following three recommendations:

1. Make Part 810s unclassified and easily accessible beyond the DoE Reading Room – publish them in the Federal Register.
2. Congress must be specific about the information it requires from the executive when an administration submits a 123 Agreement for approval; remove the use of infinite duration and extensions and implement period reviews.
3. Data on nuclear exports should be clear, complete and accurate data in order to assess the true economic value of U.S. nuclear exports rather than concealing them in national security secrecy.

**Meeting Discussion:** Henry opened the meeting by stating that one of the “sleeper national security issues” is the sharing and export of nuclear civil technology, hardware, and fuels. He quickly touches on some of the “pro-nuke” arguments for what it is a national security imperative: reactors are the coin of the realm of influence; civil reactors are what keep our naval reactor program vital; the fuels program is what makes it possible to fuel “probably our bombs.” He then noted. That those on the other end of the spectrum worry about the spread of the technology and means to make nuclear weapons. Regardless of where you fall on that spectrum, he argued that you have got to believe this is a national security concern. He then asked: How do we treat these things? Henry argues that things never were great, but have gotten significantly worse since 9/11. He argued that 9/11 was the excuse for everyone to

restrict access to information relating to the licensing of exports, the information about exports, and the information about nuclear cooperation agreement negotiations. This has resulted in poor results for our nuclear export policy. He then introduced Sharon Squassoni to make her presentation.

Ms. Squassoni, opened by saying her presentation will be less about secrecy and more about transparency, mis and dis-information, and the reliability of information. After recalling a conversation she had early on in the Trump administration with a senior official on what the plan was – frame nuclear cooperation in the context of great power competition – she began a discussion on the 2020 Energy report which she also raised in the read-ahead material. She highlighted the three basic elements of the strategy from the 2020 report: grow nuclear exports, stop all cooperation with Russia and China, and classify nuclear energy as national security. She suggested this latter element is about funding – make it about national security and get more money for and from the Pentagon – and secrecy. After a side-bar discussion on U.S. uranium supply/energy dependence, she noted that nearly all of the eight points on how U.S. national security is assured through nuclear energy do not pass the laugh test. The one exception is the need to export in order to have better awareness/control of the nonproliferation regime. It is better if the reactors are U.S. rather than Russian and Chinese, but the U.S. has not dominated the market in over 30 years.

She then summarized the discussion on Part 810s, NCMOUs and 123 Agreements from the read-ahead and closes with her recommendations.

Henry then turned the discussion back to the idea that the administration has been keeping Congress in the dark during the negotiations and then expecting to present an agreement when finalized, but notes that, after three years of noise from the Hill, it has begun to keep Congress informed during the Saudi 123 negotiations.

A workshop member who oversaw the negotiations of 123 Agreements, stated that he briefed extensively during negotiation and following negotiation before Senate and House consideration of the agreement. He held classified and unclassified briefings. He then argued that the administration adheres to the law and both parties expected the executive branch to adhere to it. He noted that they had but that was no longer the case during the Trump administration. Henry asked if there was anything that could convince the administration to follow the law, to which the workshop member responded: subpoenas, prison terms, etc. Henry argued that the language isn't actually that clear on the statutory requirements placed on the executive and asked the group member what his interpretation of the statute entails. The workshop member said that if members of the HFAC or SFRC ask for a briefing, they should be able to get a briefing to members or staff from State responsible for the negotiations. The discussion then goes into the Korea 123 Agreements and how it was presented to Congress.

Henry then pressed the workshop member to expand on what he thinks “currently and fully informed” should operationally entail. The workshop member stated that it would be wise for the administration to offer briefings, as the Obama administration sometimes did. Give Congress the option of saying yes we want this, or call us later when you have more details. When Congress does request it, then it is legally required.

Pointing to a discussion in the chat, Henry raised the question on whether civil nuclear transactions are things that need to be highly classified, or classified at all. Should the licensing of nuclear exports be classified? He states the law is clear that it has to be made public. Then the question arises as to how much information should the licenses have in them? What should be classified?

One workshop member noted that when he was at the Energy Department, he approved an 810 authorization that was so proliferation sensitive and proprietary, they did not even inform Congress what the technology was that was being transferred, though they did make the 810 authorization available without the specifics.

The discussion then turned to the lack of clearance/access for the majority of Hill staffers and the difficulty for them to get information that would inform their policy recommendations for their bosses. It was also noted that, in one of the workshop member's opinion, there was very little about civil nuclear transactions that need to be classified. One working group member then asked if there was a way to separate out policy and process from sources/methods when there is an actual need to classify some of these transactions. Squassoni first commented that the Hill doesn't have access to secure spaces like the executive branch does, and this leads to access issues and why the Hill doesn't get as many clearances or access to highly classified information. She then asked how can a Part 810 authorization itself be classified because of proliferation sensitivity when the actual transfer itself is ok? If it is good enough to go to another country, we can't be that concerned about proliferation issues.

The question was again raised about what needs to be classified and why, and then what actions are being taken to address that. Henry responded, this is the action, this exercise is trying to address those issues. However, the meeting closed out without getting greater clarity on the underlying questions of what specifically would need to be classified in this realm at what level, and how they relate to U.S. national security.

---



## **Keeping Atoms for Peace from Being Overshadowed by Secrecy: The Case of Nuclear Exports**

### **Meeting Memo from Sharon Squassoni**

**Summary:** There is increasingly less transparency about nuclear cooperation agreements, export licensing, export controls and the value of exports from the U.S. nuclear industry. There is also less information made available to the public about nuclear proliferation trends. It will become increasingly difficult for policymakers and outside experts to connect the dots between what the U.S. is subsidizing, exporting, and how it is being used or misused by partners and competitors alike to reduce or exacerbate proliferation. The U.S. Congress and the next administration can make changes to return to or increase transparency and thereby vastly improve policymaking capabilities.

### **Introduction**

In the age of endless tweeting and instantaneous posting of sensitive information, not to mention inadvertent releases of information, it is hard to imagine any area of public life that is experiencing a decline in transparency. The nuclear power sector has historically and consistently opted for the “glass half full” perspective, projecting far more optimistic outcomes than it has been able to deliver.<sup>3</sup>

Recent decisions by the U.S. government have further decreased the amount of reliable information available to the public and to Congress. The impetus to restrict information springs from the desire to promote nuclear exports at the expense of critical reviews. That desire is aided, quite consciously, by the promotion of the commercial nuclear industry as essential to national security.<sup>4</sup> This has had the counter-intuitive effect of streamlining export licensing and reviews of nuclear cooperation agreements.

In April 2020, the Department of Energy released the “Restoring America’s Competitive Nuclear Energy Advantage,” a report produced by the White House’s Nuclear Fuel Working

---

3. From early U.S. projections of nuclear electricity being “too cheap to meter” to IAEA rosy growth scenarios, to individual countries’ unrealistic targets for growth, it is the exceptional forecast that is accurate. Some of the early enthusiasm in the United States can be attributed to unfamiliarity with the challenges of scaling up nuclear power. As those challenges became more apparent over time, enthusiasm shifted to protect the nuclear industry from criticism and to bolster negative public opinion.

4. The argument suggests that if the nuclear weapons enterprise depends on a vibrant commercial nuclear industry and that commercial industry depends on exports because the U.S. itself is not building many new nuclear power plants, then national security requires U.S. to export new nuclear reactors overseas.

Group. The strategy explicitly claimed (on the cover) to assure U.S. national security through nuclear energy and listed eight national security reasons underpinning the strategy:

1. Uranium is a critical mineral (a departure from precedent)
2. Importance of nuclear energy for resilient electricity/critical infrastructure
3. DoD needs nuclear power for forward operating installations (also new)
4. Dependence on global nonproliferation and safety, which the U.S. champions
5. 5. Importance of foreign policy relationships (cemented by nuclear cooperation)
6. 6. LEU for tritium production for nuclear weapons and HEU for naval reactors (previously reliant upon hundreds of tons of stockpiled HEU)
7. Assured uranium supplies (also new)
8. Civilian workforce base.

The strategy has four objectives: provide immediate financial support/subsidies to U.S. uranium mining and the front end of the fuel cycle; decrease permitting and regulatory burdens on industry in the front end; support advanced technology and empower U.S. export competitiveness.<sup>5</sup> In this last category of empowering U.S. exports, there were eight individual tasks, several of which are relevant to this discussion. One was to “increase efficiencies in the export processes and adoption of 123 agreements to open new markets for exports of U.S. civil nuclear energy”; a second and third focused on opening up investment and financing for exports (under the International Development Finance Corporation, formerly OPIC) and a fourth was to expand civil nuclear international cooperation programs.

For the purposes of this paper, the big impact of these policies has been to push nuclear cooperation to the sidelines of 123 agreements, with the following impacts:

- more secrecy about Part 810 authorizations, designed to protect firms, not U.S. nonproliferation interests
- more secrecy about 123 agreements and less information to Congress
- more secrecy about nuclear exports and their value

---

5. Streamlining regulations on the front end amounts to overturning the ban on uranium mining on protected lands, including around the Grand Canyon.

## **Part 810s**

With respect to increased efficiencies relative to 123 agreements, the strategy declared that “Consistent with the process improvement achieved in 2019 for Part 810 applications, the USG will ensure that high standards, consistent with U.S. law are maintained while investigating methods to further increase efficiency in the processes for each.”

What was the process improvement for Part 810 in 2019? Faster processing of Part 810s, which means looser restrictions around the export of nuclear technology and assistance to countries with which the U.S. may not have a full nuclear cooperation agreement.<sup>6</sup> There are two ways to achieve faster processing: put more countries in the general authorization category or process specific authorization requests more quickly.<sup>7</sup> The first approach is harder – only three countries are on the general authorization list that do not have Section 123 agreements with the United States and all three formerly had agreements that have expired – Chile, Colombia and Mexico.

The second approach, which is to process specific authorizations more quickly, is apparently the one that saw improvement in 2019. According to the annual report to Congress on Transfers of Civil Nuclear Technology (a requirement of Section 3136 (e) of the FY16 NDAA; PL 114-92), the Department of Energy cut its approval time of Part 810 requests in half in 2019. However, the report to Congress gives no information regarding kinds of technology or information, countries, or suppliers.<sup>8</sup> Much of the work is done by DoE, determining whether a recipient country has met 10 requirements, mostly related to whether the U.S. has assurances from and the recipient has honored its nonproliferation commitments and treaty obligations. One factor is whether comparable assistance and technology is available from other sources (and here, the number of nuclear suitors Saudi Arabia has is likely to come into play). The State Department must concur and the NRC must be consulted. There is no current requirement to inform Congress. However, the code of federal regulations states that (10 CFR 810.9 (e)) within a month of granting a specific authorization, a copy of the Secretary of Energy’s determination “may be provided to any person requesting it at DoE’s Public Reading Room,

---

6. For an excellent primer on Part 810 authorizations, see Paul Kerr and Marybeth Nikitin, “Nuclear Cooperation: Part 810 authorizations, available at: <https://crsreports.congress.gov/product/pdf/IF/IF11183>

7. Part 810 of the Code of Federal Regulations (10 CFR 810) controls the export of nuclear technology and assistance in two ways: some activities are “generally authorized” by the Secretary of Energy and thereby require no further authorization under Part 810 by DOE prior to engaging in such activities. For activities and/or destinations that are not generally authorized, Part 810 requires a “specific authorization” by the Secretary. Part 810 also details a process to apply for specific authorization from the Secretary and specifies the reporting requirements for generally and specifically authorized activities subject to Part 810. Violations of section 57 b. of the AEA and Part 810 may result in revocation, suspension, or modification of authorizations, pursuant to 10 CFR 810.10, as well as criminal penalties, pursuant to 10 CFR 810.15.

8. See Department of Energy, Transfers of Civil Nuclear Technology, Report to Congress, April 2020, available at: <https://www.energy.gov/sites/prod/files/2020/04/f74/Final%20-%20EXEC-2019-000810%20Transfers%20of%20Civil%20Nuclear%20Technology%20Report.pdf>

unless the applicant submits information demonstrating that public disclosure will cause substantial harm to its competitive position.

Between 2017 and 2019, the Secretary of Energy authorized eight technology and information transfers under Part 810 (special authorizations) to Saudi Arabia, reportedly to facilitate negotiations regarding a nuclear cooperation agreement. Unlike previous Part 810 authorizations, which DoE made available to read at its headquarters, these were kept secret. Congressman Brad Sherman requested Secretary of State Pompeo to release the company names, but there is no public record of this. Several of these transfers occurred after the murder of Jamal Kashoggi and after Crown Prince Mohamed Bin Salman told CBS News in 2018 that the kingdom would develop nuclear weapons if its rival Iran did.

According to NNSA, companies requested that the authorizations were kept secret to protect proprietary information.<sup>9</sup> According to the NRC, the dates of the requests from DoE to review the special authorizations were: 2017 (Nov 3); 2018 (Jan 5, 9; Feb 12; May 18; June 20; Oct 23) and 2019 (January 22).<sup>10</sup> Given the extraordinary comments from Saudi officials regarding their intentions to meet Iranian proliferation with their own proliferation, their recently exposed activities regarding uranium mining and conversion reportedly with Chinese help, and their steadfast refusal to bring their safeguards agreement up to current, accepted standards, DoE's interpretation of the law to protect proprietary interests over nonproliferation is inimical to U.S. interests.

## **Section 123 Agreements**

Over decades, the executive branch has acted to minimize scrutiny of nuclear cooperation agreements in the following ways:

- a. Consultation comes at the end of the negotiating process, with a final copy of the signed agreement to approve. This was not the intent of the Atomic Energy Act.
- b. The nonproliferation assessments required by law have become increasingly pro forma, with some even failing to mention former nuclear weapons programs in recipient countries.

---

9. Timothy Gardner, "US approved secret nuclear power work for Saudi Arabia," Reuters, March 27, 2019, available at: <https://www.reuters.com/article/us-usa-saudi-nuclear/u-s-approved-secretnuclear-power-work-for-saudi-arabia-idUSKCN1R82MG>

10. NCR responses to request from Senator Chris Van Hollen on NRC approval of DoE Part 810 authorizations to Saudi Arabia, available on <https://www.nrc.gov/docs/ML1910/ML19108A014.pdf>

- c. The adoption of rolling extensions and unlimited duration treaties without any requirement for periodic review.<sup>11</sup>

The text of many U.S. nuclear cooperation agreements had been available prior to the Trump administration on the DoE website. This is no longer the case. The DoE/NE website now shows a map of countries that have Section 123 agreements with the U.S. and there is a list of those countries with the expiration dates of the agreements (not updated).<sup>12</sup>

Not being able to compare the texts of 123 agreements makes it more difficult for anyone to question or criticize U.S. policy. For example, the U.S. executive branch has stated it would seek restrictions on enrichment and reprocessing (the two technologies used to create fissile material for peaceful nuclear fuel or for a nuclear weapons) on a case-by-case basis. Without having access to U.S. agreements with countries in the Middle East (e.g., the UAE and Egypt) or, in fact, all U.S. agreements, it would be difficult to know that the U.S. has a specific policy to ensure that states in the Middle East rely on the international market for fuel, rather than developing their own enrichment or reprocessing capabilities (regardless of whether the U.S. cooperates in such). The texts of 123 agreements can be found in the Congressional Record, but this is hardly a user-friendly option.

More importantly, in early 2019, the U.S. State Department announced a new strategic approach to nuclear cooperation agreements. It was not clear whether the Nuclear Cooperation MOUs are meant to supplant Section 123 agreements or merely pave the way for easier negotiations. According to Assistant Secretary of State Chris Ford, the MOUs should build strategic ties with the US, its experts, industry and cutting-edge researchers about how best to tailor future opportunities to its specific needs. Ford told a Hudson Institute audience that “We would use these ties to help states build their own infrastructure for the responsible use of nuclear energy and technology and adopt best practices in nuclear safety, security, and nonproliferation, including regulatory oversight.”

Apparently, the solution to cumbersome 123 negotiations is ad-hoc nuclear cooperation MOUs to get a foot in the door and the U.S. public and Congress will have no idea which companies or countries this is occurring in.

In addition, one of the traditional routes for keeping an eye on foreign nuclear technology development – international nuclear cooperation through DoE – appears to be, from budget

---

11. Sharon Squassoni, “Civilian Nuclear Cooperation Agreements: Enhancing Our Nonproliferation Standards,” Testimony before the Senate Committee on Foreign Relations, 20 January 2014 “Nuclear Cooperation and Nonproliferation: Reconciling Commerce and Security,” Testimony before House Foreign Affairs Committee, September 24, 2010.

12. Comically, the International Trade Administration (Department of Commerce) guide for exports has an entire section devoted civil nuclear exports (<https://www.export.gov/industries/civil-nuclear>) that redirects the user to PM/Director of Defense Trade Controls website for 123 agreements, despite the fact that PM has no jurisdiction over 123 agreements.

documents, severely cut back in the FY21 budget. The DoE Office of Nuclear Energy website shows updates as recent as October 14, 2020 regarding funding for advanced reactor projects, but here's what hasn't been updated:

- The website of the Office of International Nuclear Energy and Cooperation has not been updated to reflect the halt in cooperation with Russia or China (although the FY21 budget reflects a cut of \$3M for international nuclear energy cooperation)
- International Nuclear Energy Research Initiative (I-NERI) under the Nuclear Energy division of the Department of Energy stopped publishing annual reports on the website in 2015

### **Value of Nuclear Exports/Jobs**

The U.S. nuclear industry often markets itself as a source of high-paying, skilled jobs, whether in promoting nuclear power in domestic markets or to promote foreign exports. The Nuclear Energy Institute (lobbyist for nuclear energy industry with some foreign firms) contends on its website that a single nuclear power plant generates more jobs than any other type of electricity generation station.<sup>13</sup> To support that statement, NEI claims that each plant employs 500 to 1000 workers; construction at peak requires 3500 workers; salaries are 20% higher than for other electricity generating plants; and each plant creates \$40M in labor income each year.

These numbers are hard to reconcile with the U.S. Bureau of Labor Statistics data from 2017, which claim a total of 6,010 nuclear power operator jobs in the United States. In 2019, there were 35,500 power plant operators and 5300 nuclear power plant operators, which suggests that npp operators occupied 12% of power plant operator workforce while they generated 20% of U.S. electricity. From a labor-saving perspective, this is impressive, but that is the opposite view industry would like to portray. (Solar and wind probably use even fewer laborers). It is true that nuclear power reactor operators earn more (median annual wage in 2019 was \$100,530) than other power plant operators (\$81,990), probably because they need more than a high school education and must be licensed by the NRC, typically after working in the plant in an apprenticeship capacity. A 20% premium seems actually modest, considering the requirement for scheduled updates in training and certifications.

The value of nuclear exports (and the contribution of new nuclear cooperation agreements) is similarly murky. NEI estimated years ago that the nuclear export market could bring 185,000

---

13. There's no explanation for how this is calculated (whether over the lifetime of the plant or whether by comparable level of electricity generation). NPPs in the US generate large amounts of electricity because smaller sized plants are comparatively less economic (both are uneconomic in the United States, but small plants especially).

U.S. jobs and \$125 billion in revenue from 2014 to 2024. It's hard to know how "revenue" is calculated. A CRS memo, quoted in a memo released by Senator Ed Markey's office in 2014, suggested that fuel exports constituted about \$1.9 billion/year while other nuclear reactor technology (at least from 2009 to 2012) constituted about \$350 million/year.

That said, the International Trade Administration's Top Markets report for 2017 ranked the following export markets for the U.S. nuclear industry as promising:

- For new build: UK, China, India, UAE, Mexico and Poland
- For services to existing plants: China, UK, France, Canada and India
- For decommissioning work: UK, Japan, Sweden, Taiwan and Switzerland

Obviously, the UK's exit from the EU and EURATOM in January 2020 has required negotiation of a new 123 agreement with the UK, which was previously covered under the US-EURATOM treaty. A 123 agreement was submitted to Congress in May 2018 but it is not clear what its status is. However, the UK is unlikely to be a huge importer of U.S. nuclear power plants. Chinese exports have been halted as a matter of policy in October 2019 and no exports to India have materialized since the US-India nuclear deal was inked in 2005, for a variety of reasons. The U.S. still has a decent foothold in nuclear fuel sales, but some of the more recent steps by the U.S. government to promote uneconomic but domestically sourced uranium could threaten that cost-effectiveness, whether the fuel is used at home in our nuclear power plants or for overseas sales.

## **Recommendations**

1. On Part 810s: there is no reason why there should be any secrecy about what is being provided under general or specific authorizations. Making these available in the DoE Reading Room is hardly publishing the information in the Federal Register.
2. On Section 123s: Congress should be specific about the information it requires in order to make timely, informed decisions about these agreements. The use of infinite duration is bad for nonproliferation and period reviews should be implemented.
3. On nuclear exports: The U.S. government should have good data in order to be able to assess the true economic value of U.S. nuclear exports, rather than wrapping them in the national security flag.

## **LINKS TO RECOMMENDED READINGS**

- Blundering Toward Nuclear Chaos – chapter on Making Nuclear Energy Great Again – [www.globalzero.org/blundering-toward-nuclear-chaos-2020/](http://www.globalzero.org/blundering-toward-nuclear-chaos-2020/)
- Testimony on uranium as critical mineral  
<https://naturalresources.house.gov/imo/media/doc/4.%20Testimony%20-%20Sharon%20Squassoni%20-%20EMR%20Leg%20Hrg%2006.25.19.pdf>
- Testimony on 123 agreements (January 20, 2014)  
<https://www.foreign.senate.gov/hearings/section-123-civilian-nuclear-cooperation-agreements>
- CRS report on Part 810s <https://crsreports.congress.gov/product/pdf/IF/IF11183>



# National Security and Secrecy

## Working Group Series Meeting #6

December 2, 2020

**Background:** For its sixth meeting, the NPEC working group on National Security Declassification and Clearance Policy Reform invited one of the longest-serving members of the Public Interest Declassification Board (PIDB), Mr. Kenneth Wainstein. There were no read-ahead materials. According to the National Archives, the Public Interest Declassification Board was established by statute and advises the President of the United States regarding issues pertaining to national classification and declassification policy.

The PIDB is an advisory committee established by the United States Congress with the official mandate of promoting the fullest possible public access to a thorough, accurate, and reliable documentary record of significant U.S. national security decisions and activities. The PIDB advises the President and other executive branch officials on the identification, collection, review for declassification, and release of declassified records and materials of archival value. The PIDB also advises the President and other executive branch officials on policies deriving from the issuance by the President of executive orders regarding the classification and declassification of national security information.

PIDB published a report in 2020 – *A Vision for the Digital Age: Modernization of the U.S. National Security Classification and Declassification System*. PIDB argues for a need to modernize classification and declassification policies and processes as a means of “cutting costs, improving agency digital business best practices, combating over-classification, improving declassification, and establishing a transformed, credible security classification system.” It argued that the government needs a “paradigm shift, one centered on the adoption of technologies and policies to support an enterprise-level, system-of-systems approach.” To that end, the PIDB offered 10 recommendations that largely fall under the discussion areas the working group have covered, albeit perhaps more informally and theoretical. PIDB made recommendations under three headings. The first, Strategic Policy Change: How to Do It:

1. Designate an Executive Agent (EA) and Executive Committee with authorities and responsibilities for designing and implementing a transformed security classification system.
2. Organize the national security declassification community into a federated National Declassification System (NDS). Operate the NDS in a system-of-systems enterprise to streamline and modernize classification and declassification policies, processes, and technologies.

3. Empower the National Declassification Center (NDC) with the authorities and responsibilities to oversee the implementation of the NDS system-of-systems enterprise approach for managing classified information across the executive branch, and working with the originating and equity-owning agencies.

It made the following recommendation under Strategic Technology Change: How to Do It:

4. Transition to using technology, including tools and services for managing big data, artificial intelligence, machine learning, and cloud storage and retrieval, to produce systems and services which support automated classification and declassification. This transition should institutionalize research and development activities across government, incentivize private industry participation in these areas, and reform technology acquisition.

And finally, it made the following six recommendations under Immediate Impact: Near-Term Improvements:

5. Direct the Secretary of Defense, the Director of National Intelligence, and the Secretary of Energy to develop a unified or joint plan and to assist the Archivist of the United States in modernizing the systems in use across agencies for the management of classified records, including electronic records.
6. Deploy technology to support classification and declassification automation.
7. Implement secure information technology connectivity between and among all agencies managing classified information, specifically including the National Archives and Records Administration (NARA), which manages the NDC and classified records of the Presidential Libraries.
8. Empower the NDC to design and implement a process to solicit, evaluate, prioritize and sponsor topics for declassification government-wide, in consultation with the public and government agencies.
9. Develop a new model for accurately measuring security classification activities across government, including all costs associated with classification and declassification.
10. Simplify and streamline the classification system; decide how to adopt a two-tiered classification system.

**Meeting Discussion:** Mr. Wainstein stated that overclassification is easy to think of as an inherently problematic area that cannot be fixed, but does not think that is the case. This is something that can and should be fixed. It is a matter of culture, historical habit, and a matter of

being risk-averse. We need to make the case and one of the ways to do that is to identify the problems that it causes – and it causes real damage to us and the government's ability to make and execute policy. It also causes the American public to lose confidence in what we are doing. The only way it has confidence is through transparency, and “obviously, the classification system is the antithesis of transparency.” He listed several problems that overclassification causes: it is expensive – it takes a lot of money to create and maintain these classification levels and protect the information in accordance with their requirements; it causes bureaucratic problems – knowledge is power and people can use their knowledge of the classification system and the walls it sets up as a way of controlling knowledge and information; it limits the ability of thinkers of all types (whether in government, out of government, academia) to know the facts of the issues they are examining and come up with good policy and policy proposals; it runs completely counter to the historical evolution into the digital, globalized environment – with the cyber realm, information sharing is all the more critical and the expectation is that information can and will be shared otherwise partners fall behind. He said, we need to be able to communicate across all of the constituents in our law enforcement and national security effort, and in order to do that, we need to lower those walls that separate information from each other – “classification systems are running headlong into our operational needs.”

Mr. Wainstein stated that the intelligence community and our federal law enforcement can only operate as long as the American public have confidence and faith in those institutions. They need to have enough of an understanding of what these communities are doing in order to trust them to do what they need to do. In order to instill confidence, we need to do our best to push out more information. He noted that the flip side to that is, if the intelligence community and law enforcement do not push that information out to the public, then people will take it upon themselves to push that information out from the inside – the Snowdens and others of the world.

Citing all of those reasons, Mr. Wainstein argued that over-classification is causing real harm. But he noted that it is just hard for the American public and Congress to get stirred up about it without groups like NPEC and others focusing on these issues to give them a greater spotlight to underscore the seriousness of the situation.

Opening up for discussion, Henry suggested that one of the things this NPEC working group could do is put real faces on the problems of overclassification or bad clearances (clearances as a barrier for entry into bidding and competing for government work and its impact on innovation). He hoped the group could take the discussion from the general problem down to specific instances. He notes that one of the issues the working group has focused on has been the problem that Generals Hyten, Dickenson, and Raymond have focused on: how people in control of the clearance system are “killing off the space mission to some extent.” Henry asked Mr. Wainstein to address how the PIDB has fielding that question and what it makes of it. Specifically, he is concerned with special access programs and limited communication across

efforts that ultimately results in duplication of effort and overlapping missions costing the taxpayers a lot of money. Henry also asked about sharing information with allies so that our efforts complement each other – what to build, what to buy, what to operate – and achieve integration. Losing talent due to long waiting periods for clearances is also a concern.

Mr. Wainstein noted that Henry had identified some of the “more pernicious aspects of the classification system in the space area.” With respect to innovation, Mr. Wainstein noted that you see this at all levels but particularly in the space context where, to stay on the cutting edge, government is going to need to work with private industry – startup types that have the cutting-edge technology who are not necessarily the “Lockheeds” who have whole cadres of people with clearances. He stated that the more the government sticks with high clearance level demand, the more it limits its ability to get that cutting edge technology. With respect to working with allies, he noted that space is a great example. We don’t own space. We need to work with allies in space and it is hard to do that if we can’t share our technology or information with them. In terms of limiting public knowledge about what is being done – it is hard to make a case for the NSA to need certain technologies or for SPACECOM to need certain technologies if they cannot talk about the extent of the threat that is posed by our adversaries because the information about that threat is too highly classified. Mr. Wainstein referenced recent reports that quoted a high-ranking U.S. military official questioning how the U.S. was going to deter our adversaries or bad actors from doing something with our technology unless you can tell them about our space-based capability. He stated that this is a valid point and they need to understand what we can do in order to deter them from trying to harm us.

One workshop member noted that this is an extremely complicated topic and may not necessarily line up with the past roles of the PIDB, which focuses on classification and declassification. He stated that if people want to know what PIDB is focusing on, they should read the Vision Report that came out on Modernization of the Classification and Declassification System (which was distributed to the working group as a read-ahead). He said that the issue with declassification has to do with the modernization of the declassification system. NARA and the departments that deal with declassification are small and under-resourced, so there is a problem to begin with in the core of government. With regard to the clearance issue, PIDB has not generally dealt with those issues – it is a relevant issue, but not directly related to classification and declassification management. In dealing with the basic problem, this workshop member argued that “we have a giant, and almost unresolvable conundrum with regard to maintaining security on sensitive sources and methods. Often those sensitive sources and methods cost the American taxpayers billions and billions of dollars.”

He went on to argue that as the government tries to deal with the dissemination of classified information, it is trying to service “a whole host of consumers down the line.” He believed that this cannot be dealt with at the SAP/SAR level or the SCI level, and likely not even at the TS or

Secret level, and thus the creation of Sensitive But Unclassified and similar classifications to come up with constructs to push the data down to the lowest possible level using downgrading procedures, sanitization, cover/tear line. He said that is just dealing with the information in its “dynamic form.” In its “static form,” he noted, it is information that ultimately finds its way to a declassifier who is trying to deal with requirements for declassification. So, he argues, the process of declassification is “losing ground relative to not so much the classification system but the amount of classified material that is essentially being produced today by the digital age.” Without modernization of the declassification system – which he believes has a corresponding impact of assisting in the management of the classification - to deal with this digital environment, we are losing ground and will never catch up. He notes that there are demonstrated solutions – CIA and DOE have funded or encouraged some. Ultimately, he believes the onus is on the people who use the classification system at the departments and agencies who are the owners of this information to fundamentally resource classification streamlining and declassification solutions because this costs a lot of money.

The PIDB report addresses the modern system and it speaks to the promise that AI and knowledge management have for dealing with a whole class of information. It also deals with the structure of the classification system – recommends going from a 3-level classification system to a 2-level system and having an executive agent (it recommends the DNI).

Henry noted that the workshop member had spotlighted exactly what this working group is trying to address. He says that this member is making the general points that PIDB and others have made, but what needs to be done is to take specific points and define champions who can get Congress interested in addressing both specific issues and the general problems with the overall system.

Another workshop participant noted that classification is established by security guidelines/plans that each agency create. He said that citizens can ask for a mandatory declassification review, but because the review judges it against the agency’s classification guidelines, the review typically determines that the item was classified accordingly. The problem is nobody is looking at the classification guidelines. PIDB required agencies to re-examine their guides a few years ago. This workshop participant said that he had long thought that in many cases, the real problem is information is not declassified rapidly enough – it sits around until it comes up for automatic review in 25-50 years even if the classifier or owner knows that information will not be classified in 6 months. They should put that on the document. The “practical difficulty is most agencies classify to some level – when I was [in the U.S. government] it was always SCI almost automatically, they have gotten better about it and they put a lot of stuff out now at lower levels – but none of this tends to be automatic.”

Another workshop participant noted that space was a very good example of the challenges that lie ahead because it is like the classification system, which is based on a 50+ year old culture,

where everything was SCI automatically and was hyper secret. The desire to protect outweighed everything else. This participant said that what was needed first and foremost was an entirely different culture. Sustained leadership from the top driving it down, including accountability for folks that err on the side of risk avoidance as opposed to risk management. Space is a 21st Century issue we will have to deal with to maintain our advantage. The classification system is a limiting factor of that.

Henry says NPEC has argued that the front lines of strategic deterrence are leaving the gravitational pull of the Earth and drifting up to space. You cannot talk about deterrence without getting into space.

Another workshop participant decried how few of the recommendations from the PIDB over the years have been accepted and implemented. He noted that when he was in the government, the culture was “risk-management” but nobody could define that, so the default ended up being “risk-averse.” He asked what can be done so that PIDB recommendations are better received and perhaps even mandated and turned into budget appropriations? He said NARA was so ill-equipped to be able to deal with the volume of material that is coming up for review in the digital era.

Another workshop participant asked what had been effective for the PIDB when it pushes forward with its recommendations? Getting Congress or the executive branch to agree? How can we help the board push forward its recommendations?

Another workshop member noted that this is the “purest example” of an issue that does not have an owner within the U.S. government. Someone needs to own it and have responsibility. Every agency involved in national security has its own stake and unless there is a single entity designated as the leader of this effort trying to harmonize classification practices across the different agencies, you are not going to get it done. That is why the recommendation from the report that the DNI become the Executive Agent vested with responsibility for classification reform is really important.

A Hill staffer noted that the Senate Intelligence Committee recently held a hearing on the topic of declassification. The challenges were twofold: On the legislative side there are lots of committees interested in the topic. The intelligence committees are interested in protecting sources and methods. They were interested in the PIDB report to make the DNI the executive agent on this issue, but there is no consensus on that either in Congress or the executive branch. At least not that it should be the DNI. He said that the difficulty now is, it is spread across the USG. To have a clear sense of the purposes and contours for reform, there needs to be an anchor to mobilize political will and resources and there also needs to be a program in which to make reform. He said Congress is trying to make progress on this issue and they are the ones that authorized the PIDB and last year (2019) gave it a permanent authorization. There is a

vested interest in its success. But there needs to be a handle as to who in the executive branch is going to be doing this.

Another Hill staffer noted that many on the Hill are less focused on the cost of classification and the law enforcement aspect of classification, than on classification being used to conceal critical information from the public. This could be information that may not necessarily be truly classified being sent to Congress in classified form so that it could not be shared with the public because it is politically inconvenient or embarrassing, or just not giving Congress access to certain classified documents. When classification becomes a shield for accountability, it is a political and national security problem that harms the system. He stated that classification power is vested with the executive branch on a presumption of good faith, but that perhaps is not always merited.

Henry acknowledged that this issue is something that is seized on by both ends of the political spectrum.

Another workshop participant asked what the major accomplishments of the PIDB have been since its inception. Although the board was authorized in 2000, it did not really get going until late 2006. Another workshop participant noted that the PIDB has had more success on the declassification than on the classification front. Pointing to historical analyses, he stated that historians now having access to historical Presidents Daily Briefs is due to a recommendation from the board. It also recommended that the agencies conduct classification guidance reviews every couple of years, which made it into an executive order. Another success has been trying to get the government to try to prioritize records for declassification – though, admittedly, this has not been rolled out in a way the board had envisioned. Citing technological advances, he noted that the government needs to have a system that can keep up with, and catch up with, what we do now and how it will operate for the future. This is why the PIDB is trying to focus on an entirely new system with one person in charge that involves all the others who do classification work, recognizing information cannot be siloed and owned by a single agency – it needs to be shared across agencies and across to other partners in order for it to be useful and for us to maintain our advantage.

Yet another workshop member noted that the PIDB makes an argument that it is the customers – the users of the information – who need to share their opinions in a vocal manner in order to spur change. Henry asked this member who he thinks the board thinks its customers are and how many have the board heard from. This workshop member replied that the departments and agencies that deal with classification are generally involved with the PIDB. Another workshop member stated that he always believed the customer was the public and many public interest groups go to meetings. He believed one of the greatest values to those groups of the PIDB was the ability to allow the declassifiers in the agencies to explain what they are dealing with in terms of the problems they have in the process.

Henry circled back to a previous comment on whether the oversight is not what it needs to be because of the lack of clearances available to staff in Congress and asks if that also spills over into the ability to be these customers pushing to get reform.

One workshop participant replied that it may be and noted that few congressional staff have the requisite clearances, so that may impede their ability to do the oversight work on classified matters. This workshop member also noted that staff tend to have a wider range of issues that would preclude them from being able to spend the necessary amount of time to dive deeply into this issue. This would be an argument for less classification helping oversight. But this workshop member noted that in the private sector, the smaller innovative start-ups face difficulty getting involved in programs where they could make an impact because of the barrier put up by clearances and classification.



# Security Clearances – Barriers to Entry and Innovation

## Working Group Series Meeting #7

January 21, 2021

**Background:** For its seventh meeting, the NPEC working group met to discuss security clearances – specifically, how the need for security clearances and the security clearance process produces barriers to entry and innovation for smaller start-ups or those in the public sector that may be able to provide added value to the government. This idea was discussed in previous meetings and was a major theme in the working group's sixth meeting. As it was viewed as having a current operational impact, causing dysfunctions in the U.S. government's ability to secure the common good.

In preparation for the meeting, Professor Paul Bracken provided a short paper identifying the role of security clearances in defense competition and that posits a conclusion that “the cost of security clearances as a barrier to innovation will increase as advanced technologies like artificial intelligence and cloud computing are adopted, and as small and medium sized companies become an increasingly important locus of defense innovation.” The paper lays out what Mr. Bracken has identified as the two roles of security clearances. The first is to protect critical information from falling into the hands of foreign enemies. The second, he argues, is as a tool wielded as a competitive weapon by companies and governments to restrict access to programs as a method to protect a monopoly on technologies, hide embarrassing failures and wrongdoing, and increase the value of a program by nature of restricting competition. Thus, the argument goes, clearances are used as deterrents to entry by limiting competition and blocking substitute products that meet mission needs.

Mr. Bracken believes that special access clearances are a particularly “high value weapon” and argues that this can be easily proven through a simple theory: the Five Forces Model of Industry Rivalry. This theory, he states, asserts that the degree of competition is shaped by four factors:

1. **Supplier power:** This measures the ability of companies to restrict supply in order to drive up prices or to maximize some other benefit. He likens the Intelligence Community's collection programs and how their existence is limited to a small group of people.
2. **Threat of entry:** This describes the chance that a new player will enter a market. The more players, the more competition and less profit for those already in the market.

As an example, Mr. Bracken points to Amazon Web Services (AWS) entering and winning the CIA cloud computing competition in 2013. He argues AWS's largest barrier to entry was getting people with the requisite clearances to know enough to bid on the contract. High barriers to entry, he argues, keep potential rivals from bidding because they are unable to assemble the necessary skills and information to offer a competitive proposal. A corollary to this is, classification reduces the government's ability to evaluate a proposal because they are unable to speak freely with innovators who do not have the requisite clearances, thus reducing innovation. He argues AWS was only able to do this because of the vast sums of money at its disposal, but for smaller and medium-sized organizations, this would be untenable.

3. Buyer power: This deals with the ability to dictate terms to a supplier – in the government case, the ultimate buyer is a single entity (Pentagon, CIA, other IC element). This would result in high buyer power because these entities are monopsonies – single buyers. However, he argues, in the government's case, buyer power is limited because the government is not a smart buyer, overburdened by regulation and hampered by an inability to speak with outside companies if those companies do not have appropriately cleared individuals. As a result, this shields existing firms with government contracts from new competition.
4. Substitute products: These are alternative ways to meet a need or requirement. Defense examples of this include: drones as a substitute for manned aircraft, cyber neutralizing a target instead of a missile strike, and lasers killing satellites. But in order to analyze where a substitute might be possible, an outsider would need to know enough about the existing technologies. The current security clearance system, Mr. Bracken argues, is built on a need-to-know basis “for when technologies operated in independent vertical silos,” however, this is no longer the case.

Mr. Bracken's paper makes two conclusions: First, clearances have multiple roles that need to be understood, and second, that these impediments to innovation will become a much bigger problem in the future than they are now. He states there are two reasons for this, with the first being that the defense and intelligence system in the United States is becoming more interconnected. The second is that the locus of defense innovation has shifted to small and medium-sized enterprises that are highly specialized and technical. These enterprises have a narrow ability to discover defense needs because they do not possess a breadth of knowledge or clearances to work outside of their restricted domains.

**Meeting Discussion:** Mr. Bracken began with a synopsis of the basic argument looking at security clearances from their strategic use. His argument, as stated in his memo, is that classification is used to protect information from falling into the wrong hands, but also

governments or corporations using them strategically to get what they want – to block out others, to create deterrence to entry (particularly when it comes to technological innovation), to cover mistakes, and to maximize bureaucratic control. He then discussed the Five Forces Model – breaking competition down into five forces (rivalry) – and how it is applicable to the security clearance dynamic. He reiterates the costs of security clearances hurting the U.S. are going to increase in the future. He argued we are moving into network technologies, outsourcing the innovation, noting that Apple does not create all of the apps, it opens the platform through APIs and the marketplace. He concluded by suggesting the Pentagon look at innovation in terms of the tiers of the defense industry. The locus of innovation is shifting in a relative sense to the small and medium-sized enterprises, which have a higher barrier to entry and less supply power. If we want to increase the level of innovation in the defense industry and intelligence worlds, the way to do that is to focus on things like clearances as a deterrent to entry and explore the fundamental question of innovation (who gets what?).

Henry asked Mr. Bracken to elaborate on having the Pentagon do a study on this issue. Bracken said he had asked that they look to conduct a study on innovation from the point of view that they look at who gets what from the subprime contractor, sub-subprime and go down as many layers as you can go to explore data collection which would get at this particular program. But nobody wanted to do it – probably because they are sensitive to it.

One workshop participant said he was intrigued by doing a possible study. He asked if elements of the Intelligence Community and elements of the Defense Department (and perhaps other agencies) are trying to reach out to small innovative start-ups and to bring their innovation in despite the classification barriers and to what extent Mr. Bracken considered this. He also asked how great the challenge might be for small and medium-sized companies to establish their clearance bona fides with a particular agency. Often times, he says, they stumble because they run into their own classification issues – they may have worked on special access programs (SAP), but because of the nature of those, they cannot present an accurate depiction of the innovative work they have completed because of compartmentation. He asked Mr. Bracken to what extent that complicates the use of the Five Forces Model.

Mr. Bracken noted that the first point is a very important one that has saved us in the 21st century. He says in the wake of 9/11, the NSA did a really good job in trying to change their ecosystem by really going out and looking for new innovations. If you are a government official, going to the small and medium-sized enterprises is important. On the second point, he noted that there is a lot of institutionalization that goes on. He thought that people are doing interesting work but have been so bureaucratized into security clearances and honoring the rules and regulations, that much of the federal acquisition in-house staff has developed into a compliance organization. He suggested the government create a short executive education course on these issues to demonstrate to people inside the system that there is more they can do by looking at case studies that have done precisely that.

One workshop participant then asked about the increasing use of sub-primaries – he noted that a lot of these sub-primary contractors are really just primaries that have different parts of the action. He also asked whether one of the problems is that we have innovative people who want to get involved in defense or intelligence issues, but they rarely have the cybersecurity infrastructure that would make them reliable partners for some of these sensitive programs. It is expensive for companies to come up to the capacity that these projects would require.

Mr. Bracken agreed that what we are seeing in recent years is that one of the big primary contractors bid as a sub-tier player to another primary contractor. The relationships are getting increasingly complicated. With respect to the security infrastructure and cybersecurity concerns, he says this is exactly what he fears. Larger companies will use this to beat down the smaller companies and bring down the prices and lowering their profitability so it will be a deterrent to entry. He noted that he had no answers to that. Some, we may have to just live with.

Another workshop member highlighted two other aspects of barriers to entry in the national security space: Building out and maintaining SCIFs to the appropriate levels is costly. The other is the contract vehicles. Those who can get it through the door can push others out of the way and then others want to hop on that vehicle. The ones well-positioned to get on those vehicles are the larger contractors. Mr. Bracken said he had not thought about the SCIF requirement. He wondered if there are ways to cut the price on these secure facilities and if there have been studies done on this. With respect to the contract vehicles, it is a complex world and it is hard to go through that process. He had no answers for this, but agreed it is a point to consider.

Another workshop participant stated that the problem is even bigger than we all think. The entire system was built in the 1950s and even the notion of what is classified deserves to be looked at because the government will want to take something in the commercial sector and classify it. In addition to clearances, it is the whole notion of what is a secret, how long does it need to be protected, can commercial encryption protect that information, and how do you share it. He says it came up in Afghanistan and Iraq a lot – base locations may have been classified, but service delivery people would necessarily know where they are. So, it presents an odd dichotomy. This workshop member said we have that kind of dichotomy today with start-ups and other companies. He noted that studies in DC brings awareness, but doesn't bring change. He recommended a BRAC-like process. The entire system is risk-averse. Mr. Bracken said that he is not as pessimistic as some. There are many studies on how to incorporate artificial intelligence and cloud computing that may be able to bring about big changes in the current system.

Another workshop participant noted that the situation is worse than being presented. The government has been trying to fix this problem, but there are a lot of issues that haven't even

been discussed. It is often difficult to understand what the government requirements are – what are they trying to solve and what are the solution sets they are looking for? There is no real horizon-scanning, unlike in the UK where the MOD has a horizon-scanning department (going out and finding out what innovation is out there). The amount of investment required is a real barrier to entry and it is what it is and we need some innovation and new ways to think about this. Horizon-scanning is an interesting way to do this.

Yet another workshop participant asked if it is possible for the government to create a safe harbor legally for small firms if they undertook to apply certain procedures. Then, would they be regarded as trustworthy or would that create too much of a risk as a single-point failure.

One workshop member asked about hype-cycles in start-up companies and how that might interact with all of the over-classification impediments.

Mr. Bracken replied that the hype-cycle is the exaggerated infatuation with a particular technology or idea (AI as an example today). It has some analytical content. People have done statistical studies of the hype around different technologies and how they collapse after a few years and have factored this into when you should make an investment to avoid going into the peak. But this should be well known to government agencies looking for innovation.

One other workshop member noted that the defense innovation units have been stood up to bring promising, small firms into the fold to help facilitate innovation. He noted one of the problems they have reportedly faced is that a lot of the Silicon Valley innovators don't want to go through the hassle of getting a security clearance and felt it was too intrusive.

---

## **Security Clearances: Barriers to Entry and Defense Innovation**

### **Meeting Memo from Paul Bracken**

This paper analyzes security clearances in a nontraditional way. Namely, that clearances are a significant barrier to innovation in defense technology and strategy. To show how clearances impede innovation in the defense industry I use a simple theory that is taught in every business school in the country.

The paper concludes that the cost of security clearances as a barrier to innovation will increase as advanced network technologies like AI and cloud computing are adopted, and as small and medium sized companies become an increasingly important locus of defense innovation.

## **The Role of Security Clearances**

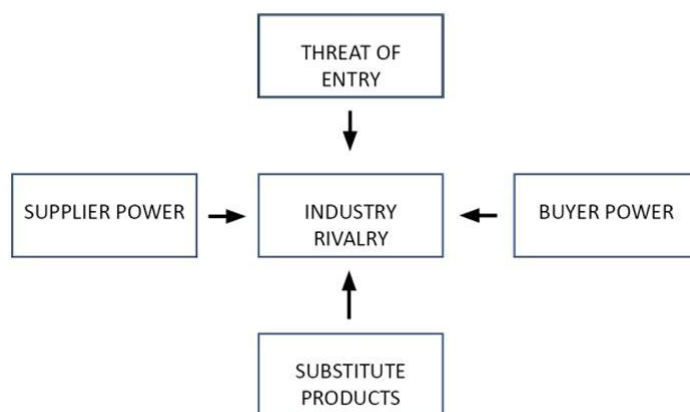
Security clearances have two roles. One is to protect critical information from falling into the hands of foreign enemies. But clearances have another use as well. Companies and government agencies use them as a competitive weapon to restrict access to programs in order to protect a monopoly on technologies, to hide embarrassing failures and wrong doing, and to increase the value of a program by restricting competition. Clearances are used as deterrents to entry, to limit competition, and to block substitute products that meet mission needs.

There are two things going on in the classification process. One is a valid effort to prevent information or technology from falling into the hands of those who would harm the United States. The other is as part of a competitive strategy in the marketplace and for bureaucratic infighting in the government.

## **Security Clearances in Defense Competition**

In the defense and intelligence marketplace clearances are a key competitive weapon. Special access clearances are a particularly high value weapon. This is readily seen using some simple theory. This theory, called the Five Forces Model, is taught in every business school in the United States and is the most widely used framework in the management consulting industry. What I had never realized before applying the theory to the subject at hand is just how negative the impact of clearances is on quashing innovation.

The Five Forces Model shown below describes the intensity of competition for any industry. Here, think of industry as made up of distinct markets, e.g., drones, cyber, military aircraft, AI, cloud computing, or data analytics.



**THE FIVE FORCES MODEL OF INDUSTRY RIVALRY**

The factor in the center of the figure, industry rivalry, is the degree of competition. This could range qualitatively from low to medium to high. Or, it could be measured quantitatively, as profit, EBITDA, or ROI. The theory asserts that the degree of competition is shaped by four factors.

Supplier power measures the ability of companies to restrict supply in order to drive up prices or to maximize some other benefit. Supplier power suppresses innovation because a supplier with power has little reason to innovate, given they are in a controlling position. Or the supplier may choose to reinforce their power by withholding information. The intelligence community may have collection programs whose existence is limited to a small group of people. In the 1998 Kosovo War a senior NATO commander was told of a collection program he did not know existed only after the war started. Had he known of it beforehand he would have changed his campaign plan considerably. The innovation that didn't happen in this case was in strategy, not in technology.

Threat of entry describes the chance that a new player will enter a market. If a new entrant does come in, it obviously increases competition, and thereby lowers profits for those already in the market. A good example is Amazon Web Services (AWS) entering the CIA cloud computing competition in 2013 and beating out IBM. The largest barrier to entry AWS faced was getting people who had the necessary clearances to know enough to bid on this contract. High barriers to entry keep potential rivals from bidding on a contract because they can't easily assemble the necessary skills and information to offer a competitive proposal. For intelligence this is especially critical because it keeps rivals (like AWS) away from a particular market. More, it reduces a government agency's ability to evaluate a proposal because they cannot freely speak with innovators who do not have the appropriate clearances. This, obviously, reduces innovation.

The AWS win over IBM in 2013 is an interesting case because it required the significant backing of a large new player, Amazon, to win the contract. It is doubtful that a small or medium sized company could have displaced IBM. Even with truly superior cloud technology a medium or small firm would have found it difficult to enter the market. Amazon with its deep pockets could do this. Most challengers could not.

One way to deal with the barrier to entry problem is for a "broker" who does understand the government's needs, and who also has the clearances to speak with outside suppliers, i.e., new innovators. Defense private equity (PE) and VC firms have partners who are retired from various agencies and the military services. The PE firm tracks the world of technology. The goal is to spot opportunities in order to link private business outsiders with government insiders. It's a valuable service, which threatens long standing suppliers to the government. The PE's strategy is to spruce up small companies by linking them with new opportunities inside

the government, markets which they never could discover on their own because they lack the knowledge and special access clearances.

Valuation of small and medium size enterprises by PE firms is contained in an investment banking “book” which details the assets of the company. The balance sheet, audited financials, physical assets, and the company’s intangible assets are in it. This book has an appendix listing the number of employees with TS/SCI clearances and special compartmented clearances. The more of these the better. It’s a measure of a firm’s intellectual property (IP) and it has significant positive impact on valuation. Companies without a large set of clearances are at a disadvantage, both in raising investor capital and in the potential for bidding on new business which requires them.

Buyer power deals with the ability to dictate terms to suppliers. Here, the ultimate buyer is a single entity, like the Pentagon, or a three letter agency. In theory, then, buyer power is high because these are what are called monopsonies, a single buyer.

In practice however, buyer power is limited because government is not a smart buyer. It is hemmed in by complex federal regulations. Those inside the government find it difficult to even speak with outside companies if they aren’t adequately cleared. This has the effect of shielding existing firms from new competition. The AWS win over IBM was a major surprise to most industry observers since IBM was so thoroughly entrenched in the Federal acquisition system. Nonetheless, AWS had a more innovative approach and won the CIA contract. This win catapulted Amazon’s cloud business into leadership in the global cloud computing market.

Substitute products are alternative ways to meet a need or requirement. Uber, for example, is an alternative to automobile ownership. Streaming video substitutes for cable TV. Defense examples include drones as a substitute for manned aircraft. Cyber can neutralize a target instead of a missile strike. Lasers can kill a satellite. Today, substitution is especially important for innovation because there are so many new possibilities arising from all of the new technologies.

But to analyze these substitution possibilities one first needs to know enough about the different technologies. The current security clearance system is built on a need to know basis, for an era when technologies operated in independent vertical silos. This is no longer the case with networked technologies, or with many different (substitute) ways to meet a requirement.

## **Conclusions**

Two conclusions come out of this discussion. First, clearances have multiple roles and this needs to be understood. They are used for business and bureaucratic competitive advantage as



well as to protect national security. Here, clearances have a serious negative effect on innovation. This includes strategy as well as technology innovation.

Second, these impediments to innovation will become a much bigger problem in the future than they are now. There are two reasons for this. First, the defense and intelligence system of the United States is becoming more interconnected. Networks are the name of the game. To plug into these networks, one needs to know about the interfaces that link the different subsystems. These are highly classified, but even more, are moving toward greater complexity for cybersecurity reasons. Cyber is the most highly classified area in defense today, like nuclear weapon secrets in the 1950s. This trend will provide a strong boost to supplier power, and it will make deterrents to entry greater.

Another reason clearances and innovation will become more important in the future is that the locus of defense innovation has shifted to a considerable degree to small and medium size enterprises. These are the small firms in Silicon Valley, northern Virginia, Austin, around Route. 128 in Boston, and elsewhere. They tend to be highly specialized and technical. And they have a quite narrow ability to discover defense needs because they don't have a breadth of knowledge or clearances to work outside of their restricted domain.

The larger defense companies can leverage their informational advantage, especially clearances, to squeeze these firms. The big firm says to the small one "Look, we don't care how great your new technology is. We've cornered the clearances and access to NSA -- and you haven't. Cut your price -- or you're out of the contract." Especially in a networked technology world, the small firm needs the larger one as it's the only gateway to large projects.

For a long time, I've urged DoD to do a study which asks a simple question: do large defense companies -- the lead systems integrators -- take too much? Are they crushing innovation in the lower tier suppliers? Today I would modify the question slightly to include the new big technology companies entering defense, and the PE and VC firms too. But the thrust of my question is the same. I've never found any interest by DoD in this most fundamental question of innovation: Who gets what?

A final point is worth making. The definition of "innovation" is usually misconstrued to mean something that is new and better. But this isn't a good definition. Innovation requires two things: something new and better, and someone willing to pay for it. It needs a buyer. The use of clearances to shape and protect a market, deter entry, or to control information for bureaucratic power reasons, is rarely considered in national innovation policy. This has to change if the United States is to leverage its immense technological potential into real military advantage.

# Are Australia's Classification Reforms a Model to Follow?

## Working Group Series Meeting #8

February 18, 2021

**Background:** For the NPEC working group's eighth meeting, a Representative from Australia's Department of Foreign Affairs and Trade provided participants with a copy of the Australian Government's [Protective Security Policy Framework](#). This Framework "defines the Australian Government's security classifications and associated handling protections." In it, it details how to handle sensitive and security classified information, including: identifying sensitive and security classified information; limiting disclosure or access to sensitive and security information to certain personnel; transferring and transmitting information by means which deter and detect unauthorized access; storing and using information securely; and, destroying and disposing of information by secure means.

The Government of Australia implemented reforms to its classification system in order to simplify the existing system. Of the major changes, the system went from having four categories of security classifications to three (keeping Top Secret, Secret and Protected, while eliminating Protected). It established an ambitious timeframe for the transition – rolling out the reforms in October 2018 with a goal of full implementation by October 2020. During the transition phase, beginning January 2019, the Australian Government agencies started to accept and receive emails under the new systems, with a requirement that all entities must ensure that their systems did not block emails marked under either the old or new system. Also, during this transition period, entities were instructed to: educate personnel on the new reforms; shift to marking documents with the new classification standards; and grandfather their current holdings of classified or dissemination limiting marker (DLM) material (though noting existing holdings need not be reclassified and that historical handling protections remained in place). Personnel during this transition were allowed to send and receive emails under either the old or new classification system through internal communications, but when dealing with external communications, they could send communications under the old or new system, but must receive communications under the old and new system.

Under this timeline, the old classification system would cease in October 2020, at which point entities were prohibited from sending or receiving emails under the old system. They were required to use the new classification system for both internal and external communications. The Framework also provided guidance for the transition period for each DLM and classification marking, their key dates, their replacement equivalency, and their handling restrictions.

**Meeting Discussion:** Ambassador Paul Myler from the Australian Embassy noted there were two significant phases of reform in their classification system: one in 2012, and one that just began in 2020. He noted that the 2012 reforms were probably the more significant because it removed the distinction between national security information and non-national security information. It recognized that all government information was potentially of significance and needed protection, but there was a blurring of the line between what was national security space and what was not.

The 2020 changes further narrowed down the classification levels and rationalized usage of the DLMs and other information markers. Another significant change was the removal of the unclassified option – it would now be unofficial or official. He noted that the driving objective behind this was the need to ensure information was protected but also ensure appropriate access to information in ways that “promote open and transparent democratic government, promote accountability in government policies and practices that may be subject to inappropriate or over-classification, allow external oversight of government operations and programs, and promote efficiency and economy in managing information across government.”

Ambassador Myler noted that classification framing is built around business impact categories, with the following being the main categories traditionally reserved for national security space: international relations (what impact would release of this information have on international relations); crime prevention, defense and intelligence.

He explained that when this new system intersected with COVID, interesting things began to happen. Previously, everyone tended to over classify and spend most of their time on a classified system. With the new reforms, the intention was to get more information on a lower system so that there would be greater access and information could be disseminated across all levels of government. Despite training and a concerted effort to do this at first, most reverted back to operating on a higher classification system than needed. However, once COVID began and people were unable to work at their classified stations, it forced everyone to really think harder about implementing the intended reforms and working on classifying information appropriately and in a way that ensured it could be shared across government. And this resulted in less information being shared on the higher classified system than on the lower, protected network system which everyone could access from home, without any negative impact on national security. This cultural shift was short-lived, however, as once restrictions lifted and people began going back to the office in Australia, people reverted back to old habits. This caused tension with government employees overseas who were not yet back in their office and able to access their higher-classified systems and those back in Australia who were again doing most of their work on classified stations.

Raymond Colston, Deputy Director of the Academy for Defense Intelligence at the DIA, discussed the Joint Military Intelligence Training Center (JMITC), its courses, and gave a brief

presentation to the group. Out of the 82 courses, prior to COVID, every course was classified in some form. When COVID began, they tried to find ways to make training opportunities available in unclassified form and virtual. They made no attempt to declassify course content. Instead, they looked for alternative content to use to make the same point and maintain the standards. At the time of this meeting, they were able to declassify about 23 courses and were teaching them virtually and all over the world. In the process, they also found they saved millions of dollars that they would normally have spent on travel and expenses for employees who enroll in these courses. He stressed that there was no policy decision that drove this, instead it was driven out of necessity. He stated that this type of virtual training will be here to stay, but did fear a reversion back to the old ways and culture once restrictions were lifted and things begin to operate in ways they did before COVID.

One member of the working group then mentioned how some agencies that handle intelligence or classified information had moved to implement some policies that they would otherwise not have done without a pandemic in order to ensure work still gets done but allows employees greater access to information. He noted that this reinforces that this is a cultural thing and it took a major pandemic to upend that culture.

Another working group participant questioned whether the U.S. government is taking a risk-based approach and weighing whether the need to access is greater than the need to limiting access. After the pandemic, there will be an expectation amongst national security professionals to use their mobile device or another secure-type device anytime, anywhere, or at any point. Might that be a mechanism to continue the drive toward reform?

Ambassador Myler answered yes, that mobile systems are driving a lot of this. But it isn't just mobile systems. He noted that because of COVID, there was a realization that you can share classified information over classified systems and that classified conversations may not necessarily need to occur in only SCIF facilities. Being more sensible about where the risk is and who is likely to be listening and how were factors taken into consideration. However, he noted that this is a situation that is unlikely to continue post-COVID, as everyone reverts back to old thinking.

Henry asked whether the Australian government is going to do an assessment on lessons learned from this experience. Ambassador Myler said no, that this is being looked at as exceptions to the rule, but there will be no changes to the rule. He is not sure there will be an assessment.

At this point, one workshop member recounted his time at the State Department and multiple technological shifts that altered the way in which the work was done. He noted that he saw a certain cycle that he perceived (whether a crest or dip with COVID) when technology changes. For instance, when mobile personal devices were issued, there was an increase of information being disseminated on the unclassified system. However, he stated it was obvious that people

were people less careful because they didn't want to be inconvenienced by having to go into the office to disseminate information when they could do it from the mobile device, which resulted in the release of information on an unclassified system that really should not have been unclassified. Then there was a time when people were being more careful because of some high-profile instances of unauthorized dissemination of classified information on unclassified systems. However, he noted that with COVID, there will be a return to that lax attitude. He then pointed out that some in the U.S. government were being given the authorization to use classified systems at home, given certain conditions were met, as a result of COVID.

Yet another member of the working group stated he believed that working from home is the future of the workforce and if the government is going to want to attract the top national security talent, that is going to have to be a consideration and it will have to include how they access classified information. He notes that on the industry side, there was a need to balance keeping pace with programs (which required access to classified information) with keeping the workforce safe. Amongst other things, it caused a prioritization of time and effort differently.

The working group also noted that there needs a more exclusive look on the time-value information, which is not part of the normal calculus on how things are classified. A lot of things are of no value a week after it is put out in the public. If that was brought in somehow, there could be less classified information or it could expire in a timely fashion.

Mr. Colston noted that time could be an element in the declassification process. It is currently part of the process, but options are limited and could be reformed.

---



## Security Classification Reforms

All official information requires an appropriate degree of protection—any deliberate or accidental compromise<sup>1</sup> of information could adversely affect government business. The PSPF defines the Australian Government's security classifications and associated handling protections.

### How to handle sensitive and security classified information

Key operational controls to protect sensitive and security classified information include:

- a. identifying sensitive and security classified information
  - i. with a protective marking
  - ii. by creating an auditable record of all incoming and outgoing material, transfer, copy or movements for, at a minimum, TOP SECRET information and other accountable material
- b. limiting disclosure or access to sensitive and security information to personnel with:
  - i. a demonstrated need-to-know the content of the information
  - ii. an applicable security clearance
- c. transferring and transmitting information by means which deter and detect unauthorised access
- d. storing and using information securely
- e. destroying and disposing of information by secure means.

## A. What has changed?

The reforms simplify the existing classification system as follows:

Then		Now
TOP SECRET	Security classifications	TOP SECRET
SECRET		SECRET
CONFIDENTIAL		N/A
PROTECTED		PROTECTED
Sensitive: Cabinet	DLM→Caveat	CABINET (Caveats can only be applied to security classified information, ie PROTECTED or above)
Sensitive	DLM→Information management marker	Apply classification or OFFICIAL: Sensitive and optional information management markers: <ul style="list-style-type: none"> <li>Legislative secrecy</li> <li>Personal privacy</li> <li>Legal privilege</li> </ul>
Sensitive: Personal		
Sensitive: Legal		
For Official Use Only	DLM→DLM	OFFICIAL: Sensitive
UNCLASSIFIED	Non-classification markings	OFFICIAL
UNOFFICIAL		UNOFFICIAL

These changes are reflected in the new [Email protective marking standard](#) at Annex A of the PSPF policy: Sensitive and classified information.

<sup>1</sup> Information compromise includes, but is not limited to: loss, misuse, interference, unauthorised access, unauthorised modification and unauthorised disclosure.

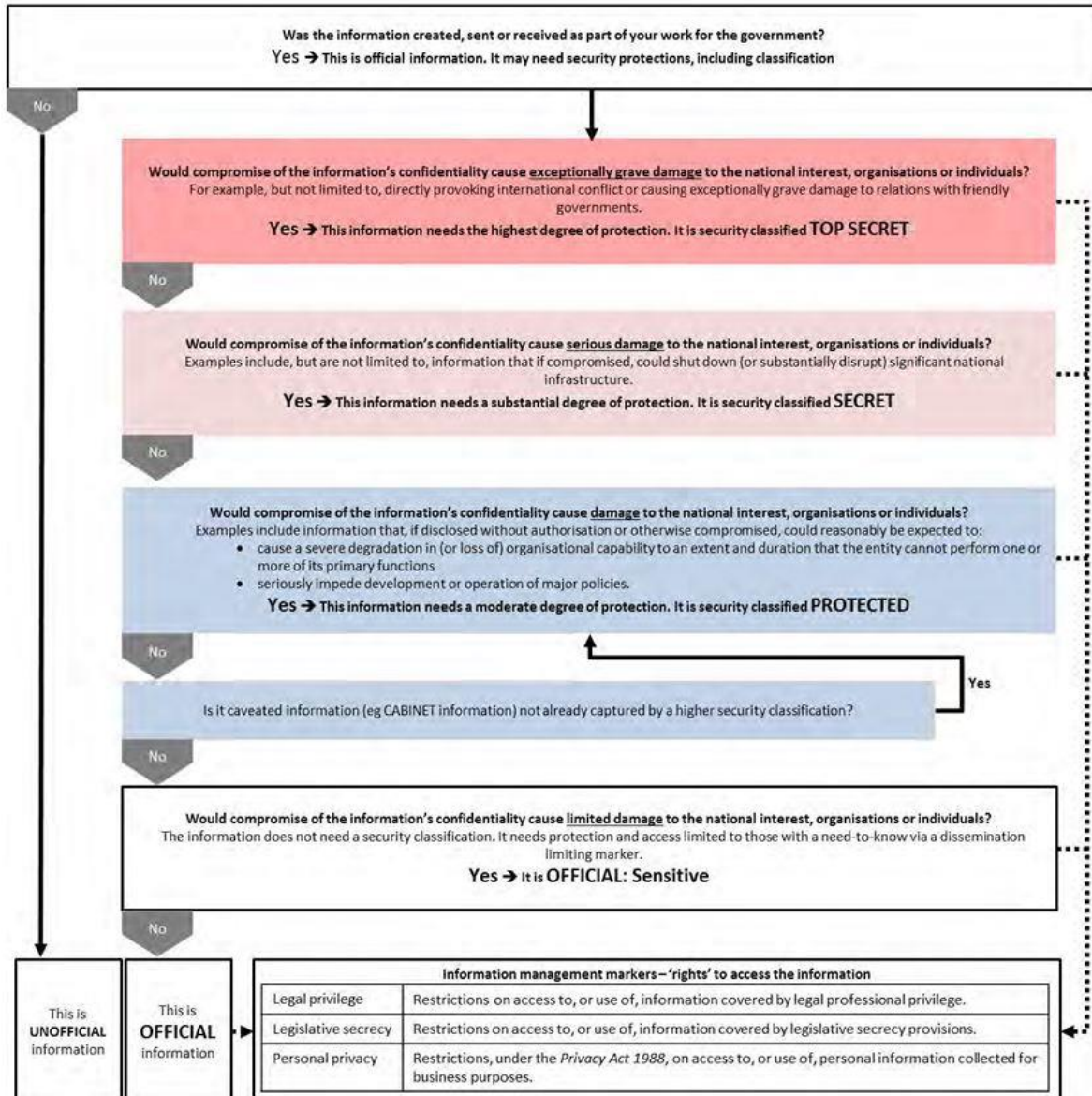


## Protective Security Policy Framework

Entities retain the option to further categorise information using other information management markers aligning with the National Archives of Australia's 'rights' property terms.

### B. Assessing whether information is sensitive or security classified<sup>2</sup>

In order to determine what protective marking to use, the originator (author/creator of the information) assesses its sensitivity or security classification by considering the potential impacts to national interest, organisations or individuals that could arise from compromise of the information's confidentiality.



<sup>2</sup> There are historical security classifications and other protective markings that no longer reflect Australian Government policy. For assistance in applying appropriate handling protections (and assessing damage to the national interest, organisations or individuals) to historical classifications, see Historical markings table.

Protective Security Policy Framework

The information management markers reflect the Australian Government Recordkeeping Metadata Standard's 'Rights' property. While categorising information content by non-security access restrictions is not mandated as a security requirement, the 'Rights' property provides a standard set of terms ensuring common understanding, consistency and interoperability across systems and government entities. For guidance, see the PSPF policy: [Access to information](#).



## Protective Security Policy Framework

## Transition timeframes and milestones

While entities can commence using the new classification system from 1 October 2018, there is an extended transition for these reforms—with full implementation required by 1 October 2020.

1 January 2019 is the collective government **start date** to accept and receive emails using the new classification system (while still retaining the ability to receive emails under the old system). Entities **must not** send and receive emails using the old classification system after 1 October 2020.

	1 October 2018	1 January 2019	1 October 2020
Implementation stage	<b>PSPF REFORMS 2018 COMMENCES</b> Transition to new system commences.	<b>NEW CLASSIFICATION SYSTEM<sup>3</sup> STARTS</b> Collective government <i>start date</i> to accept and receive emails under the new system.  All entities <b>must</b> ensure that their systems will not block emails that are marked under either the new or old system.	<b>OLD CLASSIFICATION SYSTEM<sup>4</sup> CEASES</b>  Entities <b>must not</b> send or receive emails under the old system after this date.
	Entities commence preparations to implement the new system in accordance with PSPF Policy: <a href="#">Sensitive and classified information</a> .  Entities prepare their email systems to accept messages according to the new scheme and update supporting internal ICT systems.  This includes establishing entity procedures, engaging with service providers and educating personnel on the new system.	During January 2019 to September 2020, entities: <ul style="list-style-type: none"> <li>continue to educate personnel/users on new arrangements</li> <li>shift to marking new documents with new PSPF arrangements</li> <li>grandfather current holdings of classified and DLM material—noting that existing holdings do not need to be reclassified (historical handling protections remain).</li> </ul>	After 1 October 2020, entities <b>must</b> use the new classification system for both internal and external communication.  Entities <b>must not</b> send or receive emails using markings under the old system after this date.
Internal (entity) communication	<b>Send:</b> old <b>or</b> new system <b>Receive:</b> old <b>or</b> new system	<b>Send:</b> old <b>or</b> new system <b>Receive:</b> old <b>or</b> new system	<b>Send:</b> <b>only</b> new system <b>Receive:</b> <b>only</b> new system
External communication	<b>Send :</b> <b>only</b> old system ( <b>must not</b> send externally under new system) <b>Receive:</b> <b>must</b> accept old system	<b>Send:</b> old <b>or</b> new system <b>Receive:</b> <b>must</b> receive old and new system	<b>Send:</b> <b>only</b> new system <b>Receive:</b> <b>only</b> new system

<sup>3</sup> Old classification system is the [Australian Government Security classification System](#) (PSPF 2014)

<sup>4</sup> New classification system is PSPF policy: [Sensitive and classified information](#) (PSPF 2018)

## Protective Security Policy Framework

## Markings due to cease 1 October 2020

For DLMs and classification markings due to cease on 1 October 2020, entities are strongly encouraged not to create new material using these markings after 1 January 2019. These markings must not be used after 1 October 2020.

Marking	Key dates	Replacement equivalency	Handling
CONFIDENTIAL classification	CONFIDENTIAL classification is discontinued from 1 October 2018. Recognition of the CONFIDENTIAL classification ceases on 1 October 2020.	None established. Consider the harm and apply corresponding security classification marking	Historical handling protections remain.
For Official Use Only (FOUO) dissemination limiting marker (DLM)	FOUO DLM replaced on 1 October 2018. Recognition of the FOUO DLM ceases on 1 October 2020.	FOUO is equivalent to the current OFFICIAL: Sensitive level.	Handling of FOUO information is as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive DLM	Sensitive DLM replaced on 1 October 2018. Recognition of the Sensitive DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Legislative secrecy</i> information management marker may be applied.	Handling of Sensitive information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive: Cabinet DLM	Sensitive: Cabinet DLM replaced on 1 October 2018. Recognition of the Sensitive: Cabinet DLM ceases on 1 October 2020.	The Sensitive: Cabinet DLM is equivalent to the current CABINET caveat.	Handling of Sensitive: Cabinet information is as per: a. the identified classification level and b. PSPF (and <a href="#">Security Caveats Guidelines</a> ) requirements for the CABINET caveat.
Sensitive: Legal DLM	Sensitive: Legal DLM replaced on 1 October 2018. Recognition of the Sensitive: Legal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Legal is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Legal privilege</i> information management marker may be applied.	Handling of Sensitive: Legal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.
Sensitive: Personal DLM	Sensitive: Personal DLM replaced on 1 October 2018. Recognition of the Sensitive: Personal DLM ceases on 1 October 2020.	Unless otherwise classified, Sensitive: Personal is equivalent to the current OFFICIAL: Sensitive level. The (optional) <i>Personal privacy</i> information management marker may be applied.	Handling of Sensitive: Personal information is: a. if classified, as per the identified classification level b. if not classified, as per PSPF requirements for OFFICIAL: Sensitive.

## Historical markings (ceased 1 August 2012)

Historical marking	Key dates	Current equivalency	Handling
HIGHLY PROTECTED classification	Recognition of the HIGHLY PROTECTED classification ceased on 1 August 2012.	HIGHLY PROTECTED is equivalent to the current SECRET classification.	Handling of HIGHLY PROTECTED information is as per PSPF requirements for SECRET.
RESTRICTED classification	Recognition of the RESTRICTED classification ceased on 1 August 2012.	RESTRICTED is equivalent to the current OFFICIAL: Sensitive level.	Handling of RESTRICTED information is as per PSPF requirements for OFFICIAL: Sensitive.
X-IN-CONFIDENCE classification	Recognition of the X-IN-CONFIDENCE classification ceased on 1 August 2012.	X-IN-CONFIDENCE is equivalent to the current OFFICIAL: Sensitive level.	Handling of X-IN-CONFIDENCE information is as per PSPF requirements for OFFICIAL: Sensitive.

# ITAR: A Security Clearance Barrier to Military Innovation

## Working Group Series Meeting #9

March 16, 2021

**Background:** For its ninth meeting, the NPEC working group met to discuss another barrier to technical innovation and collaboration for the U.S. government: the International Traffic in Arms Regulations (ITAR) and related technology transfer restrictions imposed on domestic and foreign high-tech firms. William Greenwalt, visiting fellow at the American Enterprise Institute, gave a presentation in which he framed ITAR as an export control problem stifling innovation.

Greenwalt provided a short read-ahead paper outlining the problem and his argument. His assertion was that “U.S. government security policies related to export controls no longer support long term national security interests and if not modified will likely result in the U.S. military falling further behind in the competition with China.” Mr. Greenwalt noted that these controls are barriers to participation in the defense market by firms in important emerging commercial fields such as artificial intelligence, robotics, quantum and advanced computing and others. He stated that companies risk their future viability and commercial sales by cooperating with the U.S. military and potentially getting their innovations “ITARed.”

He explained that “Commercial firms have found that to work with the Department of Defense requires an extensive ‘lawyering up’ to protect underlying intellectual property from being tainted by the government’s export control process. As with security classification it becomes almost impossible to get rid of an ITAR taint as it cascades down to whatever it touches.” Mr. Greenwalt provided several options to avoid this: never work with the government; first sell solutions in the commercial market to ensure that products or services are sold under the Department of Commerce’s jurisdiction rather than State Department’s; use slightly modified parts for identical items sold to the military or sell lesser versions of the technology; or develop most critical R&D offshore out of the U.S. government’s jurisdiction.

Greenwalt made the case that a new approach is needed – this is not the Cold War era and we need to get out of the Cold War mentality. He states that “Export controls were never reformed to encourage commercial participation in defense and became even more stringent in the early 2000s due to congressional concerns about cases of illegal technology transfer to China.” He noted that today’s issue is how to “incentivize a leap ahead in innovation from a different type of industrial base while facing impending inferiority” from China. He suggested that what is needed “is an understanding of the need to dominate commercial as well as military markets,

cooperation with trusted actors, and as the National Commission on AI recently reported a focus on ‘targeted’ and ‘judicious’ export controls – something that currently does not describe the existing system.”

**Meeting Discussion:** Mr. Greenwalt opened discussing his background and how he got involved in this issue and how it opened his eyes to the need for reform. He noted that barriers to Silicon Valley cooperation are the same as they are for allies due to the ITAR restrictions. After providing a history of how ITAR came about after World War II, Mr. Greenwalt explained that the Pentagon essentially destroyed the innovation system the U.S. had before getting bogged down by regulations; that innovation system carried on in Silicon Valley. The venture capital model arose out of the old radar technologies and the working with the Pentagon in that timeframe – experimentation, prototyping, testing, multiple bets. The Department of Defense viewed this as a “wasteful inefficient system” but Greenwalt disagreed arguing that it leads to massive innovation. He said there were two systems – one the Pentagon was operating on and the Silicon Valley system that commercial enterprises were operating on. Pointing to 1980 as the key date when commercial R&D overtook Defense spending on R&D for the first time, he said that the U.S. hadn’t looked back since then in terms of innovation being spurred on by the commercial sector. The military has limited innovation by controlling information and putting walls around it, while Silicon Valley is moving forward with new technologies and innovation. However, we put so many barriers in place to prevent these companies from working with Defense, with ITAR being one of the biggest.

So why hasn’t there been change to bring commercial companies in? Mr. Greenwalt noted that some efforts have been made, but we never modified security controls to the degree necessary to bring these companies in. He warned that unless we modify our system to keep pace with China, which is already modifying its system, we will be in a race that we cannot win. We need to remove and reduce various barriers – ITAR being one of them. ITAR is backward looking – “we are controlling lots of old stuff...and anything that touches that old stuff.” It also assumes U.S. military and technological dominance, which he believes may not necessarily be the case. Greenwalt noted that there is no concept of urgency or time with ITAR licenses, and it creates an incredible risk-averse atmosphere. Defense no longer has the dominance of global R&D and the resources it once had.

What is the prognosis? We are unlikely to make changes to these difficult management processes until we understand why they are there, what is their history, and a compelling case of why if we don’t change, how we are going to lose. This needs to be driven over and over again. The management processes currently are so buried down in the bureaucracy. This is both a congressional and executive branch problem. Until now it has been a fight to do nothing. The answer to the concerns we are falling behind have been to throw more money into a problem rather than address the underlying issue. Mr. Greenwalt noted that everyone is concerned about

China stealing our key intellectual property, but China may have already stolen enough that the walls we are putting up actually end up benefiting China to our and our allies' detriment.

Historically, the Defense Department has not been inclined to upgrade the country's military industrial base. But even if they did, State Department, which controls ITAR, would slow things down. Mr. Greenwalt noted that State's inability to understand what is happening in the global innovation and technological race, and why ITAR is a barrier, further entrenches the status quo. He said State has been an impediment to implementing reforms.

He argues that there needs to be a complete rebuild of the system. More effective controls around fewer things. But that requires defining "what the crown jewels are." Everyone thinks what they have is a crown jewel, but there are probably not more than 10. If we are not careful, we could destroy an important industry in the U.S. if we control it the way we control everything else – AI for example. What do we need to protect, and what are targeted and judicial controls for those types of technology? We also need to address the "ITAR taint," and deemed exports – the transfer of knowledge. You can control things by military end item, not components. You also need to reevaluate constantly – whether things are widely available or whether we need to figure out a different control process – this needs to be dynamic. But the first step in this is to establish a trusted community, and within that community, there is relief from the system and an "export control free zone of ideas." This should be expanded to our allies as well because we are not big enough to compete with China.

One group member adds that the system doesn't have the equivalent of the legal system of precedent – so it doesn't know whether or not it has made a similar decision in the past. On the point about exchanging information, just because the customer wants information shared with others in another country, you cannot do it until you get a license from the State Department. This could take months. The U.S. government customer cannot override that. Also, many restrictions don't recognize that because someone can see a technology doesn't mean it can replicate it. However, there were changes made by executive action a few years ago – particularly on communication satellites. He asked when that was and how far that action went.

Greenwalt says that was when Congress took space systems and moved it to ITAR and "hosed up" the entire commercial space world. The result was we created the European space industry as a result. So, the executive action was to move them back to free it up. But it moved it back under a different system under Commerce than what it was, so it will still be a little problematic.

A working group member notes that when the PIDB looks to declassify old documents, a big problem they run into is the DoD refusal to allow things to be declassified because they are ITAR protected. This, he says, makes little sense because the technology they protect is far outdated and the systems covered have likely not been in use by the Department for many years. He draws a parallel to this ITAR system and the classification system – products of a



different era meant to do something at the time that now hinder progress in the national security arena. Greenwalt says this is frustrating because ITAR is its own classification – it could be unclassified, but it cannot be released. This is holding us back. If we don't make this a national security issue and change our mindset in government, we are not going to see positive results.

Henry notes that there is a problem that we have seen across the working group's meeting that people do not pay any attention to – there are a lot of things that are not really classified that matter probably as much as the things that are. ITAR appears to be one of those things – something presumed too sensitive to share even though there may be no classification. This requires attention. Congress used to conduct oversight. If Congress did do its oversight, who would be responsible for that? Greenwalt says most staffers don't get this and don't understand it, so would likely ask GAO to conduct the review.

A group member says there needs to be a new arms export control act. He says it is odd that there isn't even a draft discussion bill on this. There was a draft for the export control act for Commerce for decades, and when the time came, they were ready to introduce and implement it. That aside, if there was a perfect arms export control act, he wonders who would support it in Congress? Greenwalt says this is hard and the bureaucracy will reach out to staff and tell them they can't do this, and if they do, it will be a major national security problem and it will cause problems for your boss. It is one of these things where leadership at the top of an administration needs to make this a priority and to work with staff on the Hill to do this. The problem now is you don't have a John McCain anymore – a senior go-to person to drive this. The administration could probably do 90% of this without congressional legislation. It has the authority. What authority it doesn't have, they can go to Congress and ask for it. But they will probably push it to Congress to do something, and that won't work. He says this is an anti-China solution, so hopefully Congress can pick up on that.

It was suggested that China no longer tries to steal information from the DoD servers – it goes to the venture capital-backed organizations that are driving innovation and tries to steal that information off their servers and get in on the ground floor. Greenwalt says anecdotally that seems right. The Chinese are there, talking to these companies – they don't necessarily have to invest, they identify targets and follow these companies – and the U.S. government is not identifying these companies. We need intelligence about our own economy, let alone what the Chinese are doing and we do not have it, Greenwalt says.

A group member says the Chinese process is comprehensive and agile – they are all over our innovation ecosystem from end-to-end. They don't have to invest because they get the pitch on everything. It's really discouraging. Any government bureaucracy is at a permanent competitive advantage when trying to take on a comprehensive and agile adversary like the Chinese. So, what can we do to be effective? If John McCain couldn't do this, who is the other person that could do something like this?

Greenwalt says there are some younger members of Congress that could take this mantle on and run with it. It requires a member or Senator that has been around for at least 10 years to take a project on and run with it. With respect to Silicon Valley, the studies are out there – the problems are out there. We need to create a trusted partnership with the venture capital community. Perhaps in a consortium in which you can have trusted conversations about adversarial capital. There is no current mechanism to do that. It is similar to what we need to do in information security – create trusted space to have these discussions. We also need a way to access those venture capital-backed companies. It is difficult to pull them in. CFIUS would be helpful, but the Chinese could still do a lot – those may need to be tightened further.

One group member says there are export control restrictions that apply across the board independent on whether you are sharing with DoD, so ITAR reforms may not necessarily address the problem. Greenwalt says Congress has yet to decide how to differentiate within those categories – CFIUS, ITAR, etc. We don't want to say China is the problem, so we write the laws to be more general which then picks up the Brits, the Dutch, etc. We can make it general but have a carve out for countries that are part of the trusted community. We should tier our allies and tier our enemies and that is something we don't seem to want to do from a policy perspective.

Henry closed the meeting by saying that the way out, if there is one, may require one of two things, generally: First, you need a narrative to create more of a problem in the eyes of more people that might be embarrassed enough to feel like they have to do something (maybe the China Commission needs to publish even more and have a dedicated effort to highlight the competitive disadvantage the U.S. in innovation as it relates to ITAR); second, we might want to find the areas that are most worrisome (perhaps space, cyber and AI) and then work backwards in terms of who you need to work with to address the problem and make the acquisition and development in those areas work more quickly.

---

## **ITAR and Innovation: The Export Control Problem**

### **Meeting Memo by William Greenwalt**

U.S. government security policies related to export controls no longer support long term national security interests and if not modified will likely result in the U.S. military falling further behind in the competition with China. This is because the potential application of these controls is a barrier to the participation in the defense market by some of the most innovative segments of the U.S. economy. Firms in emerging commercial fields such as AI, robotics, quantum and advanced computing, data analytics, and bioengineering fear risking their future

viability and commercial sales by cooperating with the U.S. military and potentially getting their solutions “ITARed” or covered under the International Trafficking in Arms Regulations (ITAR).

Commercial firms have found that to work with the Department of Defense requires an extensive “lawyering up” to protect underlying intellectual property from being tainted by the government’s export control process.<sup>14</sup> As with security classification it becomes almost impossible to get rid of an ITAR taint as it cascades down to whatever it touches. The easiest path to avoid this prospect is to never work with the government in the first place – particularly in a joint development process. The second-best strategy is to first sell solutions in the commercial market rather than to the U.S. government and take steps to ensure that a product or service is governed under the Department of Commerce’s jurisdiction rather than the State Department that administers ITAR. Other strategic options include using different parts numbers for identical items sold to the military, slightly modifying items to distinguish them from what is being sold commercially, or selling a lesser or dumbed down version of technology to free up a more advanced version for commercial sales. Finally, the most extreme option is to plan to develop most critical R&D offshore out of the U.S. government’s purview.

The incentives to conduct these types of strategies are not good news for the U.S. They add cost and potentially lead to inferior solutions on U.S. military items, but perhaps more importantly our adversaries will get first crack at these technologies in the commercial market before DOD ever does. That is a big deal when six of the most significant technologies of importance to DOD as identified in the National Defense Strategy are commercial. The U.S. now needs commercial innovation more than ever but many of these firms have little incentive to work with DOD as the benefits are not worth the costs.

A new approach is needed. To understand why, it is necessary to review the history of export controls and the pathways to past innovations. In World War II and the early Cold War, the U.S. developed first of their kind innovations – nuclear submarines, ICBMs, reconnaissance satellites, the U-2, SR-71, precision location, and eventually stealth. Once military and technological dominance with the Soviet Union was achieved though, the government began to wrap the innovation process up in a series of bureaucratic management procedures and classified it all – not in the formal sense but through an export control process where most items and knowledge while unclassified are stringently controlled. As a result, the defense industrial base narrowed to a few suppliers and was incentivized to become less innovative as DOD took on the centralized planning and oversight characteristics of its adversary.<sup>15</sup>

---

14. Our closest allies have long faced a similar set of circumstances. See: William Greenwalt, *Leveraging the National Technology Industrial Base to Address Great-Power Competition: The Imperative to Integrate Industrial Capabilities of Close Allies*, Atlantic Council, April 2019.

15. For a further review of this historical phenomenon in U.S. defense innovation see: William Greenwalt and Dan Patt, *Competing in time: Ensuring capability advantage and mission success through adaptable resource allocation*,



The U.S. faces an entirely different situation than it did in the Cold War with the Soviet Union. In that much simpler time military technology was primarily segregated from the commercial market. U.S. defense R&D dominated both quantitatively and qualitatively and the results were superior to allied and commercial technology. Unlike China today, the Soviet Union and the communist bloc pursued a policy of autarky cutting itself off from the emerging Western global market. The overarching problem for U.S. policymakers at the time was how to keep other countries from transferring specific U.S. military technology to the Soviet Union. The transfer of this technology could be managed through export controls while knowledge about these systems could be physically locked in safes or controlled through security classification.

The export control system developed in conformance with this set of facts and was relatively easy to implement when every defense part was unique and funded by the government. Then at the end of the Cold War the U.S. found it could not afford that system anymore. DOD attempted to adapt to the changing realities in the advancement of commercial technology and being overtaken by commercial R&D investment by modifying defense acquisition to support what was then known as the civil military integration (CMI) of the industrial base. As a result, in the 1990s, some commercial and military items began to be co-developed and made on the same production lines. The export control system though run out of the State Department did not effectively adapt its processes or perspectives to the mingling of defense and commercial technology. As a result, the first adopters in the commercial aircraft industry bore much of the brunt of working through the pain of the new ITAR taint that came from these CMI efforts.

Export controls were never reformed to encourage commercial participation in defense and became even more stringent in the early 2000s due to congressional concerns about cases of illegal technology transfer to China. While there have been some recent reforms in the system through the efforts of the Export Control Act of 2018, these have merely softened some of edges of previous tightening and done little to support CMI or address the new reality of a globalized industrial base dominated by dual use technologies. Past history does not imply that export controls are not needed nor that some efforts have not been successful for specific purposes. The problem today is just different than in the past which was to protect a large lead. Today's issue is how to incentivize a leap ahead in innovation from a different type of industrial base while facing impending inferiority. What will be needed is an understanding of the need to dominate commercial as well as military markets, cooperation with trusted actors, and as the National Commission on AI recently reported a focus on "targeted" and "judicious" export controls -- something that currently does not describe the existing system.

# How Advanced Technology Can Dig America Out of Its Classification Jam

## Working Group Series Meeting #10

April 28, 2021

**Background:** In the tenth meeting of the working group, program managers and developers from Sandia National Laboratories briefed the group on the Advanced Computer Tools for Identifying Classified Information (ACTICI) program. According to the presentation, “The motivation for the ACTICI program is rooted in the substantial number of digital documents requiring classification review.” The goal is to review classified information effectively and efficiently while limiting the amount of human resources required to do so. Under the current system, a trained derivative classifier is required to first interpret the classification guides and then combine that with their knowledge and background to review a document for classified information. The ACTICI program is a multi-laboratory program for developing advanced computer tools in an effort to reform how classified information is identified in electronic documents. This presentation was designed to update the working group on the program’s progress.

**Meeting Discussion:** The program manager asked that we keep the briefing and any discussion on the presentation in the NPEC working group controlled channels due to the program’s sensitivity. He did, however, share the following view graphs:

---



## Advanced Computer Tools to Identify Classified Information (ACTICI)

Heather Kraemer  
ACTICI Program Manager  
&  
John McCloud  
ACTICI Developer



### Motivation – The tsunami of records is here and getting worse

Today, existing classification staff cannot handle the huge volume of legacy paper records.  
The much larger volume of digital records reviews will be impossible without tools.

- What is in there?
- What am I missing?
- How do I connect the “dots”?
- How do I find the relevant information I need?



We need to improve the ease and speed of sensitive document reviews by human experts

2



## Basic classification process and problem

- Prerequisites:
  - A trained experienced derivative classifier
  - A classification guide or source document
- The classifier interprets the guide and with his/her inherent knowledge/background then reads/reviews a given document to understand if it contains classified information
- However, the depth of experience/knowledge of classifiers has been decreasing over time as experienced workers retire and new employees move more frequently from job to job; Second, digital information can be, and often is, more complex containing difficult to understand information relationships that can reveal classified information

3




## Overarching goals

- Long term program that delivers tools to classifiers and declassifiers that:
  - Improve the productivity of electronic review process – Be able to complete reviews in less time/cost
  - Improve the accuracy and consistency of classification decisions for each individual classifier and across many classifiers in same subject area
  - Have reviewers gain knowledge through use of tools, i.e., improve knowledge of classifiers/declassifiers so they make better decisions outside of the tool environment

ACTICI is a DOE AU-60 championed, NNSA-supported, multi-laboratory program for developing advanced computer tools to identify classified information embedded in electronic documents

4

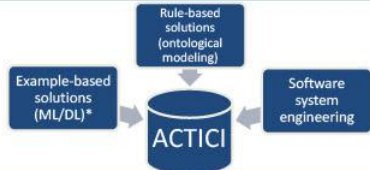


## ACTICI scope and strategies

Grow and sustain a long-term program that develops multiple tools for use by the classification community to help identify and manage classified information

- Must develop architecture, data requirements, standards and actual tools – the ACTICI Toolkit
- No expectation that human reviewers can be eliminated, rather we seek to increase reviewer productivity through software tool aids

Embrace a diversity of solutions across DOE to address challenges and modernize classification review




\*Machine Learning (ML)/Deep Learning (DL)

- Leverage expertise and existing tools to the classification mission
- Focus on digital text
- Assure tools deliver results that improve the classification system

Classification/Declassification review is an exceptionally challenging problem for computers, it is a development process that will take time to get right; however, the resources will be worth the reward


5



## Benefits of advanced computer tools

ACTICI Tools will provide

Recommendations	Classification level and category
Rationale	Words, phrases and associations that support recommendation
Provenance	Links to guide topics that support rationale



Routine Review

• Efficiency and accuracy by directing reviewer's attention to key words and phrases

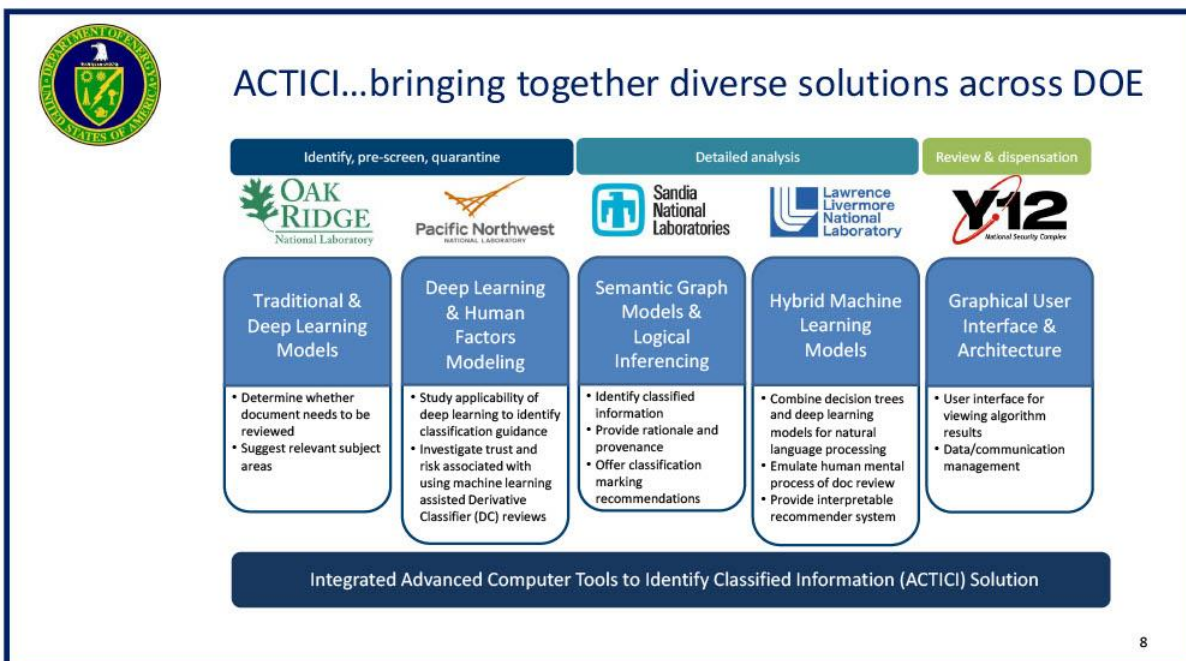
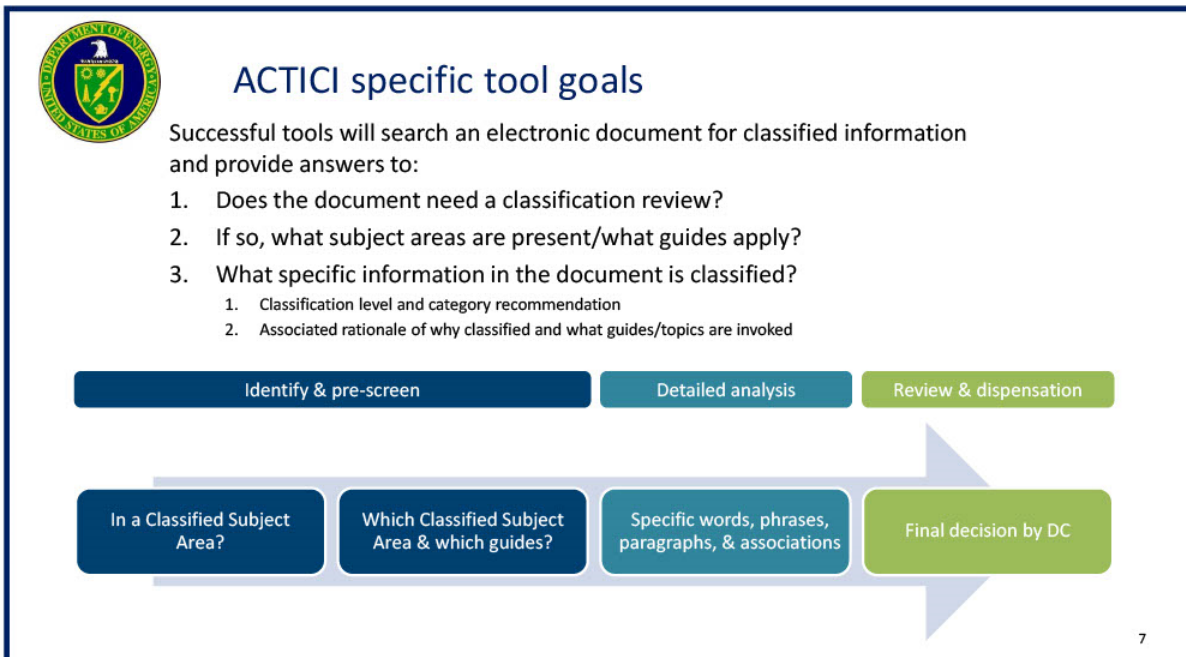
Incidents of Security Concern

• Efficiency and accuracy in assigning severity


Legacy Archives

• Efficiency and accuracy with large volume archives

6

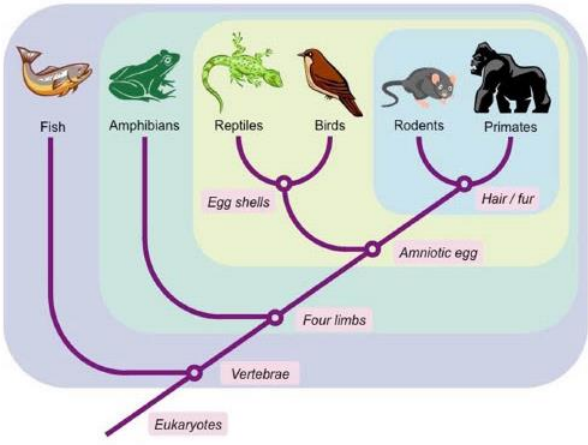







## Let us show you how this works using a dataset

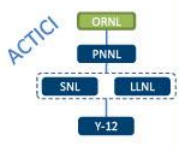
- We will use a common dataset here
  - Wikipedia has articles on everything
  - Animal Kingdom is well-suited to examples
- Our goal will be to identify sensitive information about animals
  - A Faux "Birds" guide w/example rule
    - Rule 1: Any bird that is at least 9 inches long HIGH




9




## Oak Ridge National Laboratory (ORNL) – do we need a review?



- The first thing to ask ourselves is:
  - Does a document need a review?
  - ORNL is developing this algorithm
    - Gives a Yes/No answer
    - Identifies potential Classified Subject Area (CSA)
- We *do not* base the decision to run algorithms on this step
  - This step provides a priority queue
  - Determines in what order things should be looked at by a Derivative Classifier
- Decision is based on
  - Words and related words to sensitive subject areas
  - If the algorithm says "Yes"
    - Document had many or related "sensitive" terms to subject areas
    - Likely *obviously* sensitive info in document
  - If it says "No"
    - The document had few or unrelated "sensitive" terms
    - We still check it, but push it lower on the priority queue
    - There may be subtleties requiring closer study




10

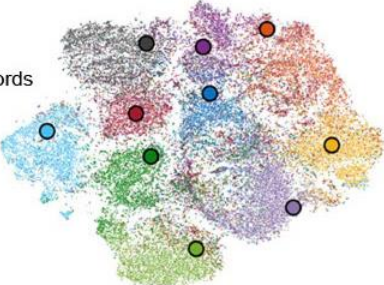


## Pacific Northwest National Laboratory (PNNL) – ACTCI

### subject matching




- There are a lot of guides
  - How do we route a document to the right Derivative Classifier?
  - How do we suggest some appropriate guides?
- PNNL** examines paragraph text:
  - Aligns the text to the subject area it might belong to
- Maps the words in the document to a cluster space of words
  - Clusters with the most words from the paragraph "win"




- Unknown
- Cats
- Dogs
- Reptiles
- Apes
- Rodents
- Amphibians
- Fish
- Birds
- Larvae
- Bacteria

11

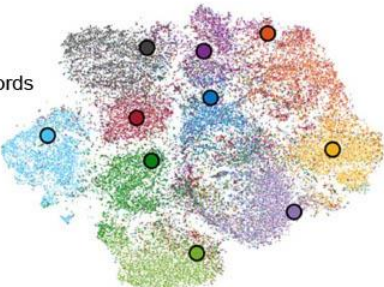


## Pacific Northwest National Laboratory (PNNL) – ACTCI

### subject matching



- There are a lot of guides
  - How do we route a document to the right Derivative Classifier?
  - How do we suggest some appropriate guides?
- PNNL** examines paragraph text:
  - Aligns the text to the subject area it might belong to
- Maps the words in the document to a cluster space of words
  - Clusters with the most words from the paragraph "win"




- Unknown
- Cats
- Dogs
- Reptiles
- Apes
- Rodents
- Amphibians
- Fish
- Birds
- Larvae
- Bacteria

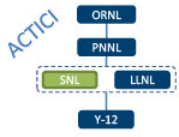
“The **shikra** is a small **raptor** (26–30 cm long) and like most other **Accipiter hawks**, this species has short rounded **wings** and a narrow and somewhat long tail. Adults are whitish on the **underside** with fine rufous bars while the **upperparts** are grey. The lower belly is less barred and the thighs are whitish. The **call** is pee-wee, the first note being higher and the second being longer. In **flight** the calls are shorter and sharper kik-ki ... kik-ki.”

12




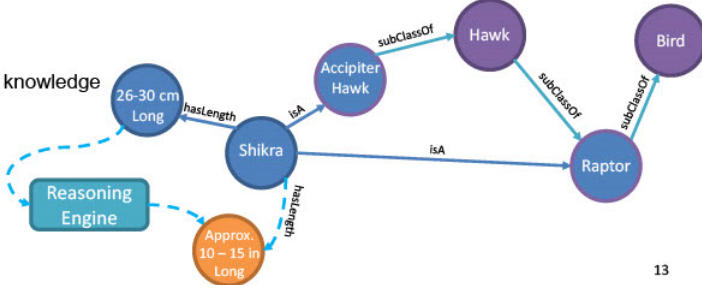


## Sandia National Laboratories (SNL) – subtleties, rules and inferencing




- We can examine the text, but what about
  - Difference between birds as pets and birds as wild predators
  - What can we infer that the document doesn't explicitly state?
- **SNL** builds inferencing through
  - Ontological knowledgebase
  - Rules and reasoning systems
- Turns text into a graphical form
  - Uses this to run rules and infer new knowledge

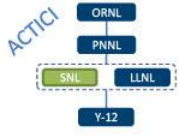
*"shikra is a small raptor (26–30 cm long) and like most other Accipiter hawks..."*

13



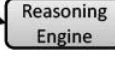
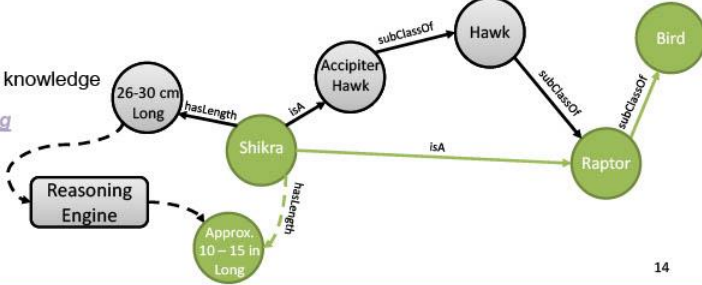
## Sandia National Laboratories (SNL) – subtleties, rules and inferencing




- We can examine the text, but what about
  - Difference between birds as pets and birds as wild predators
  - What can we infer that the document doesn't explicitly state?
- **SNL** builds inferencing through
  - Ontological knowledgebase
  - Rules and reasoning systems
- Turns text into a graphical form
  - Uses this to run rules and infer new knowledge

**Rule 1:** Any bird that is at least 9 inches long

*Rule is satisfied!* ✓

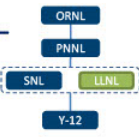



14




## Lawrence Livermore National Laboratory (LLNL) –

explainability, context and cognitive flow of DCs



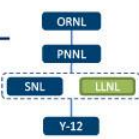
- Does an algorithm have to be a black-box?
  - Can we show how the algorithms are getting to their conclusions?
  - Can we leverage knowledge from other algorithms?
- LLNL builds an algorithm that
  - Is easy to explain with a decision tree and makes use of taxonomy/cladogram
  - Borrows from (and helps reason with) SNL ontology
  - Directly answers questions about document text sections

15



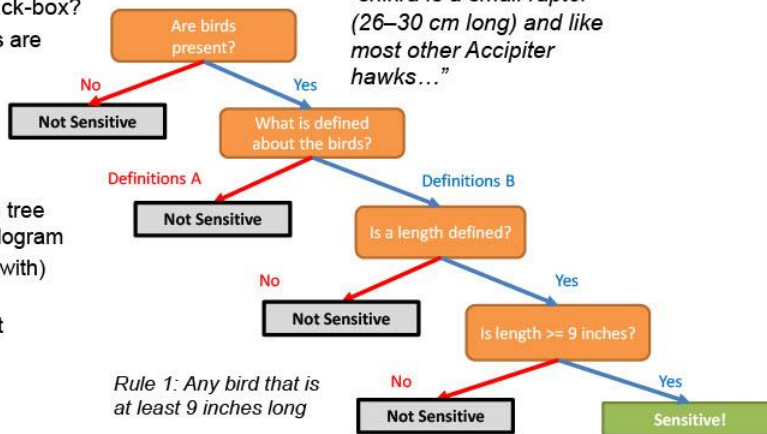
## Lawrence Livermore National Laboratory (LLNL) –

explainability, context and cognitive flow of DCs




- Does an algorithm have to be a black-box?
  - Can we show how the algorithms are getting to their conclusions?
  - Can we leverage knowledge from other algorithms?
- LLNL builds an algorithm that
  - Is easy to explain with a decision tree and makes use of taxonomy/cladogram
  - Borrows from (and helps reason with) SNL ontology
  - Directly answers questions about document text sections

*“shikra is a small raptor (26–30 cm long) and like most other Accipiter hawks...”*




**Rule 1: Any bird that is at least 9 inches long**

16



## Lawrence Livermore National Laboratory (LLNL) –

explainability, context and cognitive flow of DCs



### Directly Ask Questions of Documents

☒ Are birds present?

☒ What is defined about the birds?

☒ Is a length defined?


☒ Is length >= 9 inches??

☒ Highlight attention ☒ Underline answer

Complete!


The shikra is a small raptor, 26–30 cm long and like most other *Accipiter* hawks, this species has short rounded wings and a narrow and somewhat long tail. Adults are whitish on the underside with fine rufous bars while the upperparts are grey. The lower belly is less barred and the thighs are whitish. Males have a red iris while the females have a less red (yellowish orange) iris and brownish upperparts apart from heavier barring on the underparts. The females are slightly larger. The mesial stripe on the throat is dark but narrow. In flight the male seen from below shows a light wing lining (underwing coverts) and has blackish wing tips. When seen from above the tail bands are faintly marked on the lateral tail feathers and not as strongly marked as in the Eurasian sparrowhawk. The central tail feathers are unbanded and only have a dark terminal band. Juveniles have dark streaks and spots on the upper breast and the wing is narrowly barred while the tail has dark but narrow bands. A post juvenile transitional plumage is found with very strong barring on the contour feathers of the underside. The call is *pee-wee*, the first note being higher and the second being longer. In flight the calls are shorter and sharper *kik-ki ... kik-ki*. The Chinese sparrowhawk is somewhat similar in appearance but has swollen bright orange ceres and yellow legs with the wing tips entirely black.

17




## Y-12 National Security Complex –

review and structure results

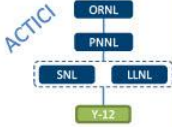


- The algorithms have done their work, but what about
  - Giving the information to the user?
  - Interaction with the results for fine-tuning by the Derivative Classifier?
- Y-12 has a solution
  - Robust Portable Document Format (PDF) viewer (handles other formats)
  - Many needed features for Derivative Classifiers
    - Algorithm-Specific Results
    - Guide Chapters Hierarchical Dropdown
    - Show/Hide Highlighting
    - Embedded Portable Document Format (PDF) Note-taking

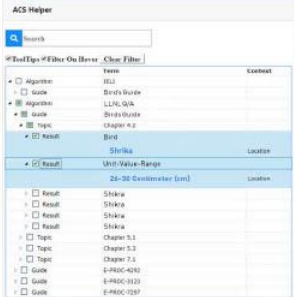

18




## Y-12 National Security Complex – review and structure results



- The algorithms have done their work, but what about
  - Giving the information to the user?
  - Interaction with the results for fine-tuning by the Derivative Classifier?
- Y-12 has a solution**
  - Robust Portable Document Format (PDF) viewer (handles other formats)
  - Many needed features for Derivative Classifiers
    - Algorithm-Specific Results
    - Guide Chapters Hierarchical Dropdown
    - Show/Hide Highlighting
    - Embedded Portable Document Format (PDF) Note-taking

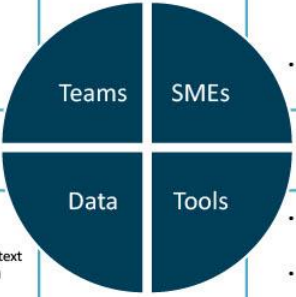



19



## ACTICI observations to date

- Labs are actively applying algorithms to DOE data
- Able to leverage some tools from academia and open source



- Experts make a key difference
- Close partnering between classification subject matter experts (SMEs) and algorithm teams produces more accurate knowledge models
- Demand for Artificial Intelligence (AI) scientist is exceeding supply

- Controlling scope is key
- Continuing challenge
- Need high-quality, large volume of text data in machine-readable format(s)
- Data needs to be balanced, with similar document structure, and annotated across classified and unclassified

- Need for tools is pervasive across DOE, NNSA, and other government agencies
- Strategic approach to manage growth and breadth of effort
- No digital collaboration space shared across the DOE complex

20





## Demonstration

21



## Accomplishments/Progress

- Developed process to automate the conversion of DOE structured classification guidance to rules for rule-based AI algorithm
- Updated tools used in directed question-answering algorithm to incorporate recent advances in open-source technology
- Evaluated and updated machine learning tools used in identifying classified subject areas
- Began assembly of a domain-specific shared data set
- Deployed “sandbox” software to each site for testing, including a user interface for display of algorithm results mapped to the original PDF.

22



Questions?

# How The National Geospatial-Intelligence Agency Controls Its Secrets: The Way Forward for Our Government?

## Working Group Series Meeting #11

September 23, 2021

### **Meeting Notes:**

NGA created a new classification management team in 2016, which looked at taking all of NGA's classification guidance and do a line-by-line review and see what is the feasibility of reducing/consolidating down to one classification guide.

Leadership said we need to modernize how we do business on the info we are protecting and how we protect it. The result was the CoNGA SCG – Consolidated NGA Security Classification Guide – and SMaRT – the Security Management Resource Tool.

Henry: From 65 to one classification guide, which suggests that at a minimum it is conceivable this can be done government-wide at a similar rate, let me ask you, how often do you review or alter your classification guide a year?

NGA: No set schedule for releasing updated versions. Review process is constant. One of the features on SMaRT is an inquiry form where users submit recommendations for additions, modifications, or deletions of line items. That is a constant flow that is coming into the team. We can get one or two a week, 15 at a time. Never stops.

Henry: What is the standard amount of time that is generally allowed for review at other agencies?

NGA: Requirement for agencies is that a guide is reviewed every 5 years by DoD guidelines.

Henry: If I want to appeal a decision, how quickly do I get an answer?

NGA: If you were to want to change a line item in the guide or appeal. Would be considered the same as what we would do to delete a line item. We would acknowledge immediately. Within the next month, request would be presented to the working group (working group is made of each OCA at the agency). Working group would evaluate the request and reach a decision of concurrence or non-concurrence. Then forwarded to the OCA. That OCA then has 30 days to make a decision from time they are presented with decision memo.

Henry: Some of us have personally experienced a review process that lingers in infinity as the number.

Henry then opens up the conversation to questions from the chat room.

Working group member: I'm involved in this with the army. They have 400 guides. What was the pushback from the community? What was the cost?

NGA: It was existing NGA employees from various mission sets across the agency that became part of this team. Original concept of SMaRT – it's basically a sharepoint. Not fancy/high-tech. Used existing resources we had in the agency. What was already existing on our systems and platforms. All done with existing personnel and technology. That's why it is really a model for others to follow. Does take dedicated leadership buy in and dedicated team. Once started, need to keep that momentum going. Process can drag on.

Working group member: How applicable is process to other IC elements to consolidate guides? What would your recommendation be? Is it transferable to others.

NGA: We've had other agencies come in and review our process. Even army. They have 500+, air force has more. They start to wring their hands when confronted with the level of challenge. Need commitment and momentum. People need to forget their day jobs and commit to the effort and put on tight timelines.

Working group member: You had top cover and leadership encouragement, but you mentioned other agencies may have equities as well. Bulk of NGA info comes from other organizations (NRO, CIA, military, commercial or civil providers). OCA is often elsewhere. Can you speak to the coordination process and how that interfaced with processes in the other organizations that may have believed they had equities and authority to make the judgments.

NGA: It is an ongoing challenge to figure out who's got the equities. NRO is one of our closest partners. We've been very successful, working with them, differentiating between what are their equities and what are our equities. They supply the data; we turn it into intelligence. Algorithms, SIG based intel, observations. Those are ours. Plus, our administrative processes, personnel info, and facility info are all ours as well. We found other agency equities were in there to give our stuff context – we decided we didn't need their equities if we did our job right. We could leave theirs out.

Working group member: How much transparency do you have into what is happening on the declassification side? Older data, etc.

NGA: Declassification issues used to be handled in the classification office. That has been segregated into its own office and basically concerned with the 25-year declassification review. They have their system. But I would agree with you that declassification and classification are



intertwined immensely. The best declassification program is an accurate classification program. We would love to automate the whole process – we have ideas about that if anyone wants to throw some money our way.

Working group member: In the 5 months you worked on this and made final presentation, how much had to be compromised and dropped off or did you get everything in there?

NGA: We settled for an 80% solution with the idea that our ongoing process would fix the other 20%. Did we have trouble in the beginning? Yeah, we had to convince the personnel in the agency that we were going from 65 to 1. We had an ad campaign, we had meetings, we had a grace period. All to sell the project after we were finished.

Working group member: Does your system apply to GEOcaps and other geospatial collection agencies?

NGA: Prefer not to talk how we handle GEOcaps here, but it's consistent with how we handle other materials.

Working group member: Sharing with other IC elements? Taking advantage of JWICS modernization efforts?

NGA: Yes, we have had agencies and other partners reach out to us. We've helped them set up their process. There are ongoing engagement and discussions.

Working group member: The use of enhancement statements (value, damage, unclassified) is a great idea. Did you talk about principals of things you were no longer going to classify in the future or strategic changes that would result in less things classified?

NGA: Absolutely. Transparency has two parts – mission, and how money is being spent. We were driven by the mission part. We realized we had to utilize the unclassified resources available outside the agency. We needed to leverage that. If we kept this suit of armor called secrecy, piled on so thick, we were incredibly protected but incredibly useless in the game of geospatial information. The attitude used to be: This is really complicated; it must be classified. We said that is not going to work anymore. We need to be judicious on where we apply secrecy. That was the main impetus. To get rid of those umbrella line items that gave the derivative authority to almost classify anything you wanted, we cut those out very quickly and refined what we were going to apply secrecy to. Higher walls around fewer secrets.

Working group member: Do you have the problem of informal process? Classification restriction that is not captured in guidance, but culturally known in the organization?

NGA: We call that classification by road. Yeah, we do our best; what can we say. In doing our best, we've empowered the NGA workforce to make these decisions. We found most people

want to follow the rules, they just want to know what the rules are. They found enhancement statements extremely helpful. No one has eliminated classification by road, but we're doing our best.

Working group member: Enhancement statements strike me as very useful. For how many lines is there information that would allow user to render something unclassified? Or how does that work?

NGA: Roughly half of the line items identify something as being classified. So, any of them will have enhancement statements. There are some scenarios where a line item will identify something as classified and there is no way to say the same thing in an unclassified manner. Don't have breakdown. But there are circumstances where it isn't possible.

Working group member: As you were developing CoNGA, did you also seek to classify at a lower level to allow greater information sharing and if so, how do you go about making those risk-based decisions?

NGA: We do have a process. It's a long process. However, we had a lot of information that was classified at TS-level that we thought needed to be reevaluated. The value was we needed to get this information to the warfighter that lives on the Secret network. If it was TS, they just don't get it. There was one category of information we reduced from TS to SECRET level. Maybe 30 line items were TS, we reduced down to about five so we could push it out to the warfighter. Process took a while and needed a lot of sign off.

Henry: What you hear here is that this process NGA accomplished is that it is not something that is plug and play. It requires buy in from the top. Would congressional interest in this instill executive interest in pushing this? That is a key question.

Working group member: I understand that a significant amount of geospatial info at the unclassified level, that is gathered by commercial sources, may actually provide greater on the ground fidelity than classified sources. This presents an interesting and somewhat confusing situation. Can you comment?

NGA: The answer is no. We can't comment.

---



## The Consolidated NGA Security Classification Guide (CoNGA SCG)

NGA GEOINT Protection Team

Approved for Public Release, 21-725

1

### CoNGA SCG Overview

- The Bottom Line on the CoNGA SCG
- Security Classification Guide Observations
- The CoNGA SCG Build Process
- CoNGA SCG Online – The Security Management Resource Tool (SMaRT)
- Conclusions and Endorsements
- CoNGA SCG and NGA GEOINT Protection

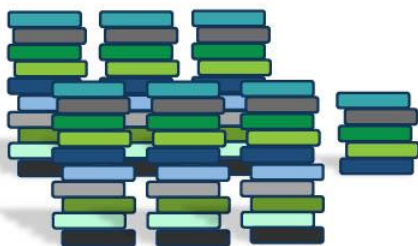


2

## The Bottom Line on the CoNGA SCG

**Purpose:** Consolidate all of the individual NGA classification guides into a single source and validate its content in keeping with NGA's current mission and functions.

### 65 Legacy SCGs



Major Deliverables

Consolidated  
NGA  
(CoNGA)  
SCG

One document that contains an updated and modernized list of NGA information (i.e., the line items).

and

Security  
Management  
Resource  
Tool (SMaRT)

An online, searchable version of the CoNGA SCG that allows users greater access and availability.



3

## Security Classification Guide Observations

### Observations & Conclusions

- 65 separate classification guides in various stages of completion.
- Long timelines (~9 months) to get a classification guide approved and signed.
- Lack of agility in updating classification guides.
- Line item redundancies, conflicting classifications, and external agency equities in NGA SCGs.

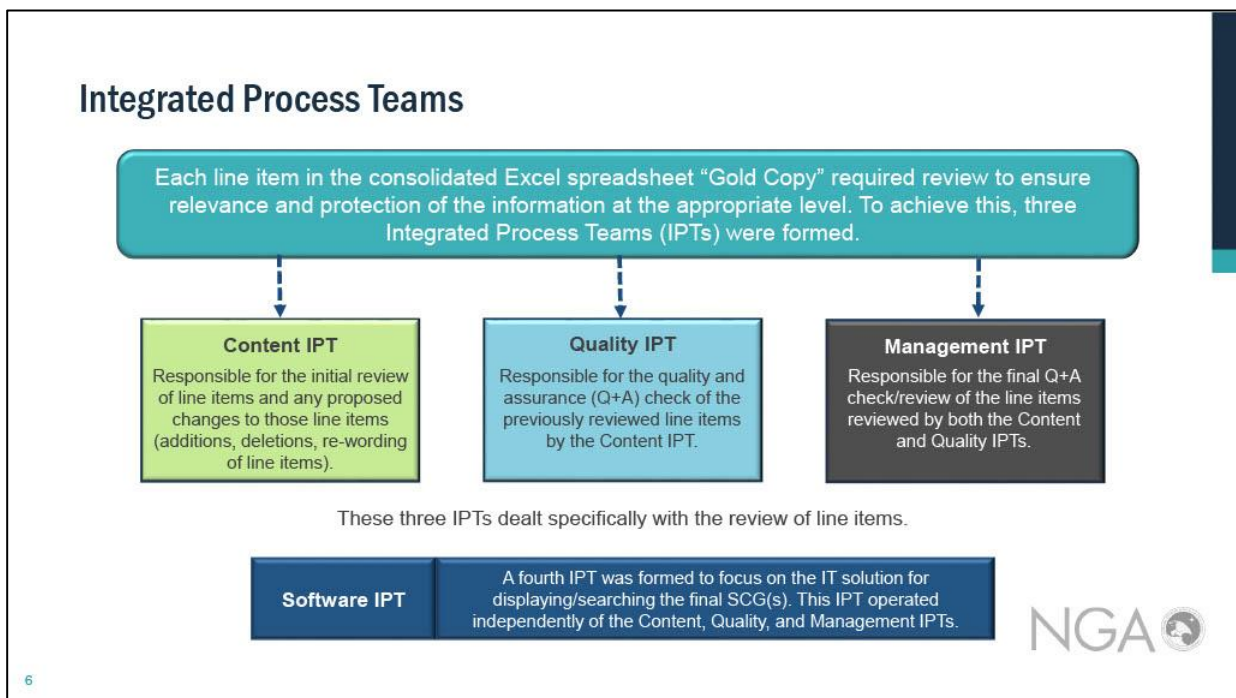
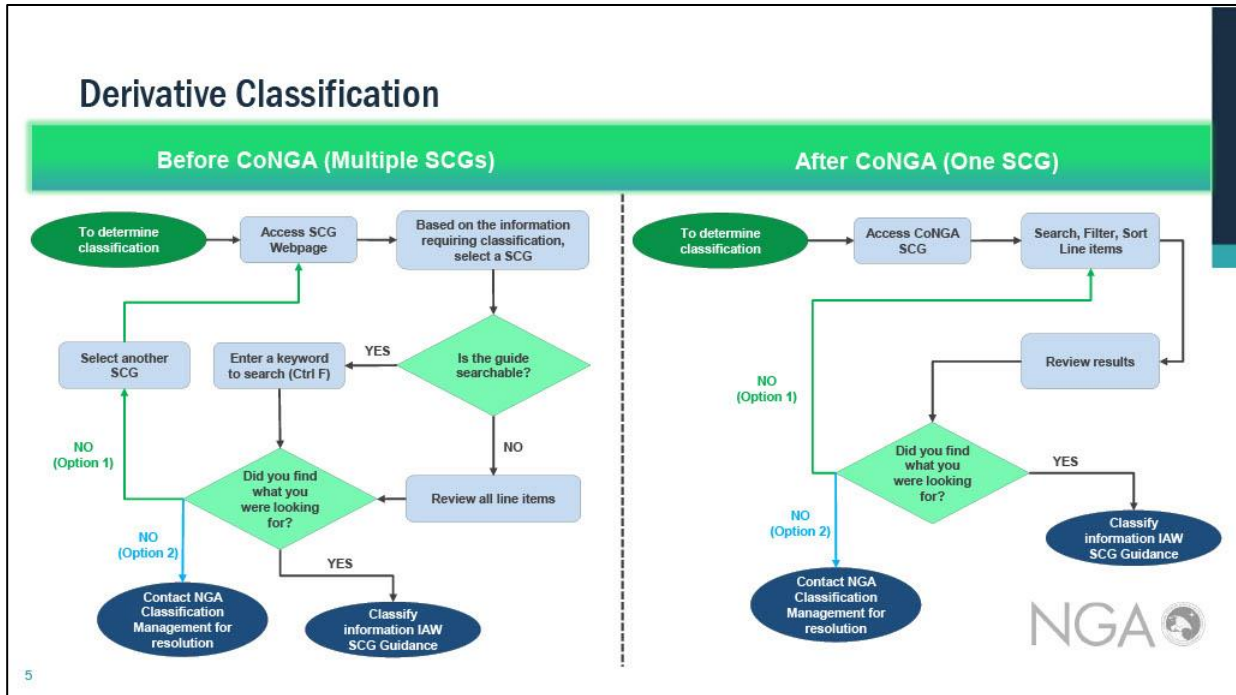
### NGA Leadership Observations & Conclusions (at the time of CoNGA creation)

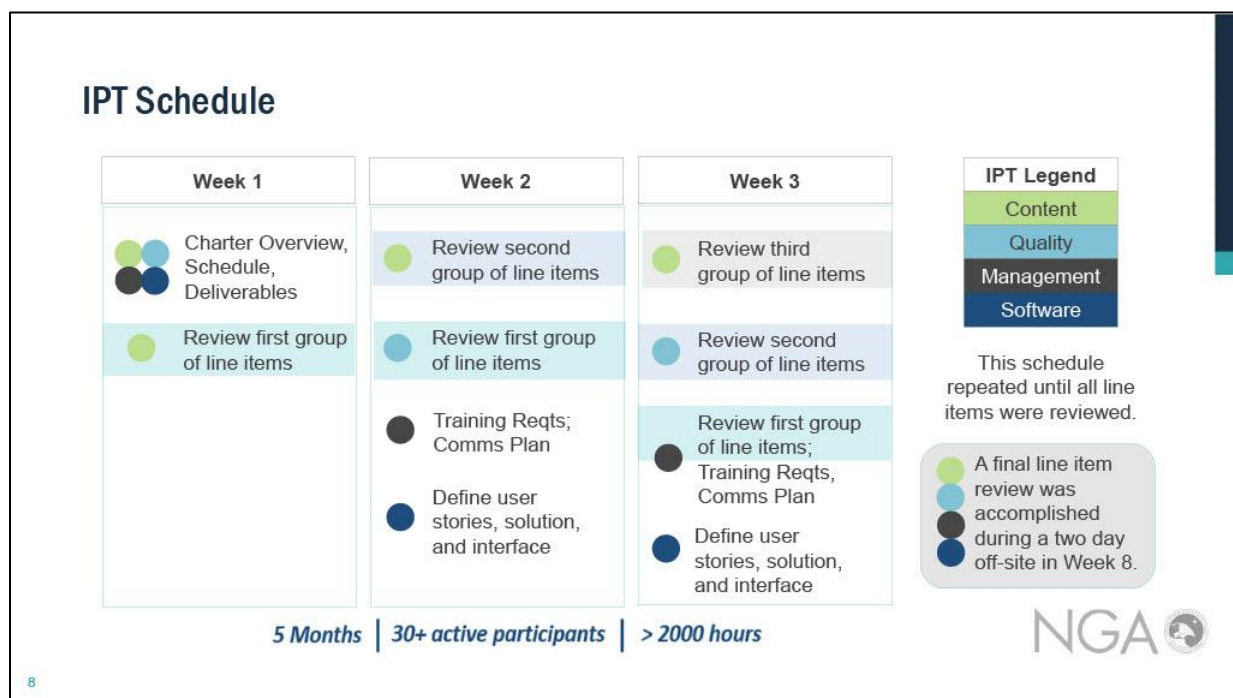
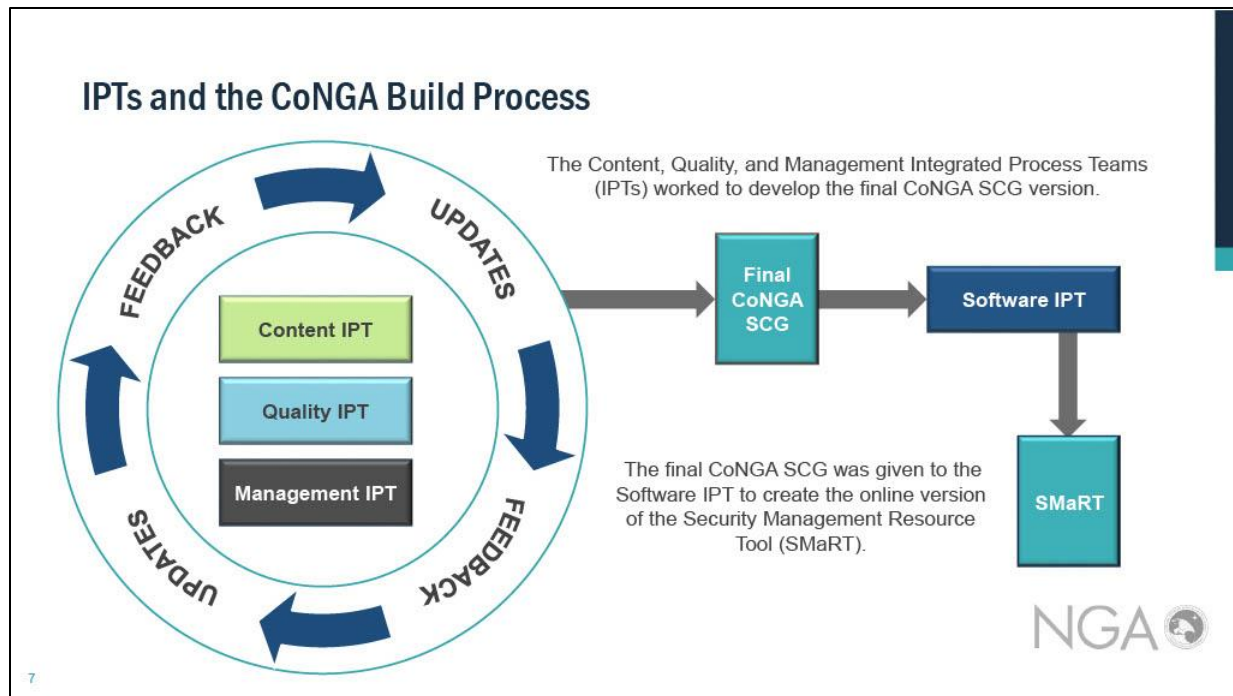
- SCGs "based on old notions of TCPED...that could make it challenging for NGA to achieve future strategic objectives (DD/NGA).
- The GEOINT SCG is more reflective of the "Cold War," not the, "current environment" (NGA/CoS).

NGA's security classification guides must be modernized.



4







## Enhancement Statements

CoNGA SCG incorporates three amplifying statements for each classified line item. These three statements are labeled: *Value*, *Damage*, and *Unclassified*.

Enhancement statements are not applicable to unclassified line items.

### VALUE

The Value statement explains why the information is being protected.

### DAMAGE

The Damage statement describes the potential impact to National Security should an unauthorized disclosure (UD) occur.

### UNCLASSIFIED

The Unclassified statement outlines how a user can address the classified line item in an unclassified manner.

Unclassified statements marked "N/A" indicate the information cannot be addressed at the unclassified level.

Enhancement statements help users: *manage risk*, *build appropriately classified products*, and *increase product dissemination*.

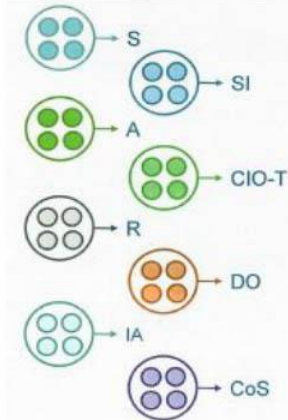


9

## CoNGA SCG Overview – Original Classification Authority (OCA) Restructure

*Before CoNGA SCG*

32 SCGs signed by different OCAs.



*After CoNGA SCG*

D/NGA-signed CoNGA SCG; Individual OCAs have authority over specific line items.

### CoNGA SCG

- Line items 1-30 (IA)
- Line items 31-75 (DO)
- Line items 76-103 (CoS)
- Line items 104-132 (SI)
- Line items 133-167 (S)
- Line items 168-211 (R)

D/NGA

*Line item numbering is for example only*



10

## CoNGA SCG Metrics

### Reduced Redundancy

**2525** SCG line items reduced

### Improved Utility

**45** Classification downgrades

**16** Line items added

**365** Line items revised to enable user derivative classification at the lowest level.

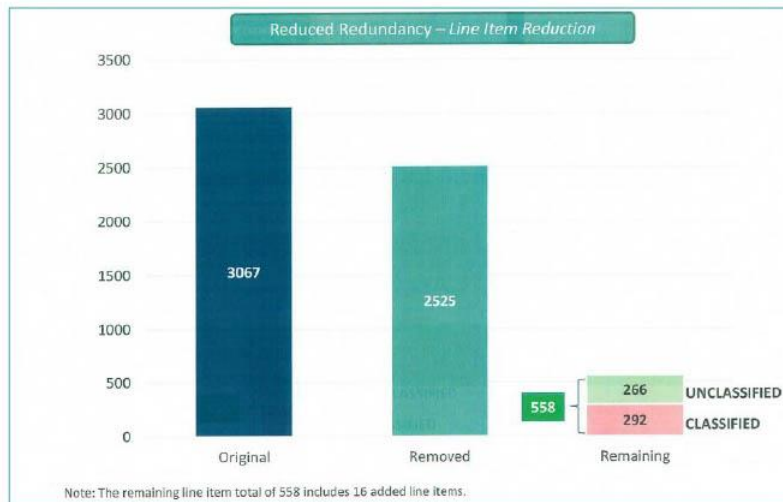
### Modernization

**292** Enhancement statements added



11

## CoNGA SCG – Reduced Redundancy



12



## CoNGA SCG – Improved Utility and Modernization



NGA

13

## CoNGA SCG – What it Will and Won't Do



### CoNGA SCG Will...

- Allow users to build products at a desired classification level
- Enable accurate classification
- Refer you to release processes and authorities
- Enhance your Derivative Classification Authority (DCA)
- Focus on GEOINT and NGA's equities.



### CoNGA SCG Won't...

- Make your information unclassified
- Make classification decisions for you
- Allow unclassified public release
- Make you an Original Classification Authority (OCA)
- Classify external agency equities

NGA

14

## CoNGA SCG Online – The Security Management Resource Tool (SMaRT)



### CORE

- Type a keyword(s) into a textbox and the system returns CoNGA SCG line items.
- Access CoNGA SCG via a web browser.
- Access to the CoNGA SCG website based on PKI (not username and password).

### SEARCH

- See search results that give at least a few lines of information per item.
- Use Boolean logic in search parameters (i.e., AND, OR, NOT, etc.).
- Perform "Advanced Search" (narrowed searches based on selected fields).

### ANCILLARY

- Quickly access a glossary of acronyms and definitions.
- Access FAQ information pertaining to how to use the CoNGA SCG.
- See announcements about recent decisions and updates.

### ENHANCEMENTS

- Links to the GEOINT Protection Team website and other resources.
- Link to a fillable SMaRT inquiry form for requesting changes to the guide.



15

## Conclusions and Endorsements

### NGA is leading the DoD and IC in Classification Management transformation

- Fully embracing the principles of the Reducing Overclassification Act.
- Enabling greater transparency and information sharing.
- Better identification and protection of the truly important information – higher walls around fewer secrets.

**Setting the scene to enable greater analytical and general user risk management and flexibility** by delivering clear and concise classification guidance to GEOINT producers and users, worldwide, 24x7.

**Making a complex task (accurate derivative classification) simpler and easy to do.**

### Positive feedback on the CoNGA SCG:

- "...Our highest possible endorsement of what NGA is doing here...extremely impressive, groundbreaking work...clearly a possible example or model for how to achieve transformation, for the IC and Nationally..." (ODNI).
- "This isn't just a concept for NGA but a necessity for DoD and the IC" (OUSD(I)).



16

## CoNGA SCG and GEOINT Protection



NGA 

17



Approved for Public Release, 21-725

# How Should Congress Manage Staff Access to Secrets

## Working Group Series Meeting #12

January 26, 2022

**Background:** The twelfth and final meeting of the working group brought the discussions full circle by focusing on one of the root issues: If Congress is meant to oversee, and ideally fix, the national security classification and security clearance processes, it first needs to get access to the information before it can begin to approach legislative fixes. At issue here is the dearth of requisite security clearances available to staff who work in Congress. The group received a presentation from an individual who served in relatively senior staff positions both in Congress and in the executive branch, who asked that his identity be protected. He argued that disparate access to classified information between similarly cleared legislative and executive branch staff often makes reform difficult. Without full access to the information, Congress is unable to get the full picture of just how the classification and security clearance processes are stifling innovation, impeding cooperation with allies, and preventing access and transparency. And without knowing where or how to fix the problem, these issues compound and it becomes a vicious cycle. The presentation explores a fundamental issue – the battle between Congress' need to know and the executive's control of classified information and what it is willing to share. The presenter and participants discussed the merits of the arguments and possible solutions moving forward.

**Meeting Discussion:** What is the problem we are trying to solve? The easy and short answer is: the disparate level of access to classified information that members of Congress and their staff have when compared to similarly cleared individuals in the executive branch. The more difficult question is: What is the appropriate amount of information, and access, Congress should have to national security information and how do we achieve that parity in access?

The presenter noted that the intent of classified information from early on was to protect and control information related to the national defense and foreign relations. And as the working group has heard over its previous 11 meetings, the reflexive over-reliance on secrecy and proclivity for over-classification has in many ways limited, or even worked against, the very problem classification was meant to solve.

The overarching concern we have is that members of Congress and their staff cannot make informed national security policy decisions if they don't have access to all the relevant information. Without access: it leaves a gap in information that could undermine the objective of the policy; it could inadvertently tie the hands of the administration and implementers,

causing unnecessary friction between the two branches; and it could limit Congress' ability to conduct proper oversight of the administration. When we say members of Congress don't have access to all the relevant information, we mean that in several ways: First, Congress is unnecessarily restricted in the number of staff made eligible for clearances; and, probably more importantly, even when members and staff are deemed eligible, the flow of relevant information is still limited to Congress.

The idea of protecting national security information and interests is not new. It may have taken different names or different forms, but the idea of protecting national security interests is practically as old as civilization itself. The Article of Confederation recognized the need to keep military and diplomatic activities secret – an idea that was carried through during the Constitutional Convention and ultimately reflected in the Constitution under Article II Section 2, which has generally been recognized as to provide the President the implied authority to control the dissemination of information related to the national defense and foreign relations.

In 1940, FDR issued Executive Order 8381 – the first ever EO dealing strictly with classification issues and really, the beginning of where our current system began. The Manhattan Project was classified under this EO. By 1951, Truman issued EO 10290 which established today's system of categories (Confidential/Secret/TS) and the rules for classifying and securing information. Since then, just about, if not every, President has issued EOs that address classification issues.

Congress really started getting into the game in 1946 when it passed the first statute dealing with classification – the Atomic Energy Act. When the National Security Act was passed in 1947, establishing the CIA, was really when we started seeing the current tension between the executive and legislative branches. The presenter notes that according to the National Archives and Records Administration's Information Security Oversight Office Report to the President (of 2017), the number of Original Classification Authority decisions in 2017 was just under 60,000 – however, nearly 50 million derivative classification decisions were made. This is hundreds and hundreds of millions of pages of classified information being produced each year. He notes that there are only about 2000 original classifiers, but there are over 4.3 million cleared individuals across the executive branch, including contractors – estimates generally put those with SCI eligibility at or above 1 million.

Now, turning to Congress, the presenter pointed out that, according to a 2020 report from the Project on Government Oversight, there were a reported 637 Senate staff with active security clearances – 353 Secret/TS and 284 TS/SCI. Each Senator is afforded two cleared staffers in their personal offices (though not at TS/SCI). If they sit on one of the national security committees, they may have an additional cleared staffer, and this individual would be eligible to access compartmented information. This will vary from Congress to Congress, but in

general, this is around about one-third of Senate offices – meaning two-thirds of the Senators do not have a staffer that has such access.

In the House, things are less clear: there is no public accounting – though, reportedly a report has been generated but not made public. But in general, each House member is afforded two cleared staffers (Secret/TS level). Certain committee staff are eligible for access to compartmented information. Given this, he notes that it would be safe to assume that there are at least twice as many staff in the House with clearances as there are in the Senate. So, in total, that means somewhere in the neighborhood of 2000 cleared staff – including staff at supporting agencies; this is not even a fraction of a percent of the number of cleared individuals.

The presenter noted that there were whispers circulating that efforts were currently underway to allow each Senator a staffer in the personal office to be eligible to access compartmented information. While he believes that is a good start, it obviously does not go far enough. Staff are still limited to what the administration chooses to provide Congress, which generally does not include: identities of intelligence sources, “methods” used in collecting and analyzing; “raw” or “lightly” evaluated intelligence, and written products tailored for the President or other high-level officials. Executive branch officials commonly cite the need to protect against “leaks” as one of the top reasons for limiting congressional access. The presenter noted from his personal experiences there were multiple occasions when colleagues stated that they don’t want to include certain information in a report or brief to Congress because they – the working level staff – were concerned about Congress leaking that information.

Of course, a common congressional concern is that administrations tend to try to bury information in classified reports because they don’t want that information becoming public. Here too, the presenter witnessed this, giving an example of a Department trying to send two versions of a report to Congress – one Secret and one unclassified. The Secret report contained only one sentence that was classified. Everything else was unclassified. He noted that, not only could this line have been rewritten so it could be used in an unclassified manner, but the entire classified report contained much more information at the unclassified level than the actual unclassified report. He was told it was done because those drafting the report preferred that information be out of public view. Unfortunately, that isn’t how this process is supposed to work.

Has Congress mishandled information in the past? Sure. But so have individuals in the executive branch. But, the presenter said we can’t put all of the blame on the executive branch here. He argues that just like in many other areas, it can be said that Congress has not been as protective over its oversight authority and has ceded much to the executive. It has even put up many of the roadblocks to access itself – from not allowing already cleared staff (detailees, etc.) to fully utilize their clearance, to not expanding access to more staff, and to not expanding secure space.

So, what is the answer? The presenter noted that this briefing was really meant to get the discussion going and that he will present a few ideas just as thought exercises to provoke discussion on how to move forward. None are a silver bullet, though some are a bare minimum of what can be done.

**In the Short Term:** Every member of Congress should be allowed to have at minimum of one TS/SCI-cleared individual. Having at least one trusted staffer that can attend briefings with, or for, them and pour over the mountain of classified documents is important. This staffer will be much more attuned to the member's interests and needs as opposed to the limited committee staff. This is certainly not going to break the system, and remember, these individuals still need to be vetted and cleared through background checks and are subject to criminal penalties should they leak sensitive information.

There could be the formation of a Classification and Security Clearance Reform Caucus. While these caucuses aren't the sexiest of options, they do provide an opportunity for like-minded members to join cause and promote their interests, tailored to the subject. At the very least, it could be a platform for discussion and education. Some may even form legislation.

Congress also needs to get serious about the issue – but in order to get serious about the issue, it first needs to understand the scope of the issue. Reports have been mandated in the past, but these are either ignored or – you guessed it – kept secret. Congress should mandate a GAO review – to be unclassified and publicly available – that details the number of clearances, disaggregated by security level, committee/office, and the resources needed to ensure appropriate access and access controls. The review should also be expanded to cover the executive branch – to include the number of SAPs, how many slots each SAP holds, and how (and why) a need to know is determined and why Congress is not “read in.”

**In the Medium Term:** Congress should get organized to look at these issues. Creating a committee to deal specifically with classification and security clearance issues would allow for broader jurisdiction than just the intelligence community. It would be a facilitator of access and would be responsible for oversight and accountability to ensure the administration is fulfilling access requests the Congress. It could also help expand workspace for cleared staff to access materials, use secure email and other communications, and brief their respective member. This would be different from the House or Senate security offices in that those offices do no accountability or oversight. Of course, Congress could also go with the Joint Intelligence Committee and implement reforms that way.

**In the Long Term:** Interoperability. The legislative and executive branch operate on different communications systems. Congress should be integrated into the same systems used by the executive branch. This would still be predicated upon the “need-to-know” so that staff are not accessing information beyond the scope of their jurisdiction but would ensure that staff are able to access products at will. This would also require Congress to create additional secure space.

---

**NPEC's National Security Classification &  
Clearance Policy Reform Working Group  
Meeting #12**

**How Should Congress Manage Staff Access to Secrets?**

*“[A] legislative body cannot legislate wisely or effectively in the absence of information respecting the conditions which the legislation is intended to affect or change; and where the legislative body does not itself possess the requisite information—which not infrequently is true—recourse must be had to others who do possess it.”* – Justice Willis Van Devanter



## What is the Problem We're Trying to Solve?

- Disparate level of access to classified information between Legislative and Executive Branches
- What is the appropriate level?
- Don't eliminate secrecy – make it more accessible
- Members cannot make the most informed decisions without access to relevant information.
  - Restricted on staff clearances
  - Restricted on what they get access to

## A (Very) Brief (and incomplete) History of Classification

- Continental Congress: Members passed resolutions obligating themselves to “consider themselves under the strongest obligations of honour” to keep the proceedings secret.
- The Article of Confederation recognized the need to keep military and diplomatic activities secret
- Constitution Article II, Section 2
- Executive Order 8381: March 1940 – the first to deal with classification
- Truman's EO 10290 in 1951 – the foundation of today's system
- 1946 – Congress gets in the act, passes the Atomic Energy Act
- Numerous EOs and statutes passed since

## Purpose of Classified Information

- Protect and control national security/defense and foreign relations
- September 11<sup>th</sup> – lack of information sharing, increased scrutiny
- Pendulum swings – reflexively over-classify (or incorrectly classify); are we working against our own interests?

## Classification by the Numbers – Executive Branch

- Nearly 2,000 individuals with Original Classification Authority
  - These individuals in turn make about 60,000 OCA decisions
  - These result in nearly 50 million derivative classification decisions
  - This creates hundreds of millions of pages of classified information
- Over 4.3 million cleared individuals, including contractors
  - Nearly, or just over, 1 million eligible for access to compartmented information

## Who's at Fault?

- **Congress and Executive Branch**
  - Executive Branch mistrust of Congress
    - Limits what Congress sees; limits access
    - Generally does not provide: identities, methods, raw or lightly evaluated, or tailored products generated for POTUS/other high-level officials
    - Often cite "leaks" – not only at the top, but staff level seem to make these decisions
  - Congress mistrust of the Administration
    - Congress believes Administrations try to bury information in classified reports
  - Congress lacks interest/engagement except when politically expedient
    - Self-imposed limits on clearances, does not allow detailees with clearances to carry those over fully, lack of secure space expansion

## Classification by the Numbers – Legislative Branch

- 2020 Repor that 637 Senate staff have active clearances
  - 353 SECRET/TS and 284 TS/SCI
    - Two cleared staff for Senator's personal office (only up to TS)
    - Extra cleared individual (TS/SCI eligible) if they sit on NatSec Committees – approximately 34
    - Certain committee staff and Leadership staff eligible for SCI
- No public reporting on House clearance numbers
  - As in Senate, two per personal office (up to TS/SCI); committee staff and Leadership staff eligible, as are certain individuals in the Legislative support agencies
  - Potentially 2,000 or so cleared individuals for Congress – just a fraction of a fraction of a percent of total cleared U.S. individuals

## Solutions?

- Expand number of cleared staff
- Understand the scope of the problem – GAO mandate report
- Caucus?
- Joint Committee? New Committee?
- Interoperability with the Executive Branch

<b>Name</b>	<b>Affiliation</b>
Steven Aftergood	Federation of American Scientists, Project on Government Secrecy
Mark Albrecht	Former National Space Council
Charles Allen	Chertoff Group
Jennifer Aquinas	Security, Special Program Oversight and Information Protection, Office of the Administrative Assistant, Office of the Secretary of the Air Force
Andrianna Backhus	Office of the Administrative Assistant, Office of the Secretary of the Air Force
Mounira Badro	Embassy of Canada, Washington, DC
Charles Ball	Threat Reduction and Arms Control, U.S. Department of Defense
Omar Bashir	Office of Senator Edward J. Markey
Rick Berger	Senate Armed Services Committee
Sharmila Bhatia	Information Security Oversight Office, National Archives and Records Administration
Michael Binder	Air Force Declassification Office, Joint Base Andrews   National Archives and Records Administration, College Park
Krista Boyd	House Committee on Oversight and Reform
Paul Bracken	Yale University
James "Jim" Bruce	RAND
Richard Buenneke	Space Policy, Office of Emerging Security Challenges, Bureau of Arms Control, Verification and Compliance, U.S. Department of State
William Burr	National Security Archive
Brooke Buskirk	Nonproliferation Policy Education Center
Daniel Calzada	Sandia National Laboratories
Pablo Carrillo	Squire Patton Boggs
Edie Chalk	U.S. Department of Energy
Seth Center	Brzezinski Institute's Project on History and Strategy, Center for Strategic and International Studies
Richard Chancellor	U.S. Department of Defense
Paul-Noel Chretien	Public Interest Declassification Board
In Bum Chun	Retired South Korean Army   Association of the United States Army (AUSA), Korea Chapter
Jaimie Clark	Senate Committee on Homeland Security and Governmental Affairs
Taylor Clausen	Office of Senator Rob Portman
Ezra Cohen	Public Interest Declassification Board
Raymond Colston	Academy of Defense Intelligence, U.S. Defense Intelligence Agency
Matthew Connelly	Columbia University
Thomas Countryman	Arms Control Association
Madeline Courvisanos	Embassy of Australia, Washington DC
Troy Cribb	Partnership for Public Service
Matthew Daniels	Center for Security and Emerging Technology, Georgetown University   Office of Net Assessment, U.S. Department of Defense
Joseph DeTrani	Former Daniel Morgan Academy Graduate School of National Security
Kevin Diamond	Office of U.S. Representative Lisa Blunt Rochester

Sharon Dondlinger	Security, Special Program Oversight and Information Protection, Office of the Administrative Assistant, Office of the Secretary of the Air Force
Michael Draper	LinQuest Corporation, SETA Support to the Space Control Division, Office of the Assistant Secretary of the Air Force for Space Acquisition, and Integration (SAF/SP)
Jaymie Durnan	The Andrew W. Marshall Foundation
Martin Faga	Former President and Chief Executive Officer, MITRE Corporation   Former Public Interest Declassification Board
Robert Fahs	Information Security Oversight Office, National Archives and Records Administration
John Ferrari	American Enterprise Institute
Brett Fetterly	Office of Senator Ben Sasse
Beth Fidler	Information Security Oversight Office, National Archives and Records Administration
Kensy Finnegan	Office of Senator Lisa Murkowski
Maria Fox	Headquarters, Air Force Material Command, Small Business Office
Brett Freedman	Senate Select Committee on Intelligence
Torrey Froscher	Independent Consultant
William "Renn" Gade	U.S. Department of Defense
John Galer	National Security Space, Aerospace Industries Association
Stephen Garber	Office of the Assistant Secretary of the Air Force for Space Acquisition and Integration, Policy & Integration Division
Frank Garcia	U.S. House of Representatives Permanent Select Committee on Intelligence
Patricia Gaviria	Brookings Fellow, House Foreign Affairs Subcommittee on Oversight and Investigations
Carly George	Sandia National Laboratories
Caroline Goodson	Office of Representative James Langevin
Bruce Goodwin	Lawrence Livermore National Laboratory
Christian Goos	Information Security Oversight Office, National Archives and Records Administration
William Greenwalt	American Enterprise Institute
Ben Grinham	British Defence Staff, British Embassy
Einar Gustafson	Royal Norwegian Embassy, Washington, DC
Jeffrey Harris	Former Lockheed Martin   Former National Reconnaissance Office   Former Air Force for Space
Pete Hays	Falcon Research
Taylor Hilliker	Information Security Branch, Office of Security, U.S. National Geospatial-Intelligence Agency
Adam Howard	Office of the Historian, Foreign Service Institute, U.S. Department of State
Robert Hunter	U.S. Senate Foreign Relations Committee
Richard Immerman	U.S. Department of State
William Inboden	Clements Center, University of Texas at Austin
Robert Jervis	Columbia University
Alexander Joel	Office of Civil Liberties, Privacy and Transparency, Office of the Director of National Intelligence

Alec Johnson	Office of Senator Christopher Murphy
Zach Keck	House Foreign Affairs Subcommittee on Oversight and Investigations
Scott Kemp	MIT Laboratory for Nuclear Security and Policy
Anastasia Kouloganes	U.S. Government Accountability Office
Annie Kowalewski	Senate Foreign Relations Committee
Heather Kraemer	Sandia National Laboratories
John Lauder	Independent Consultant
Richard Lawless	New Magellan Ventures International, LLC.
Michael G. Lawrence	Public Interest Declassification Board
Brian Leitzke	Defense Fellow
Theresa Lou	House Foreign Affairs Committee
Bailey Martin	Nonproliferation Policy Education Center
Thomas Mahnken	Center for Strategic and Budgetary Assessments
Ellen McCarthy	Former Bureau of Intelligence and Research, U.S. Department of State
John McCloud	Sandia National Laboratories
Jeffrey Mellott	Air Force Material Command Small Business, Department of the Air Force
Brandon Mendoza	Office of U.S. Representative Sara Jacobs
William “Jeff” Merrell	Rolls-Royce North America
Ian Merritt	Office of U.S. Representative Chuck Fleischmann
Stephanie Mitchell	Defense Fellow, U.S. Air Force
Charles “Chas” Morrison	Office of Representative Mike Gallagher
Mark Mozena	Planet
Mark Myers	Air Force Life Cycle Management Center, Air Force Material Command
Paul Myler	Embassy of Australia, Washington DC
Bryan Oklin	Information Security Oversight Office, National Archives and Records Administration
Christian Ostermann	History and Public Policy Program, Wilson Center
Greg Pannoni	Information Security Oversight Office, National Archives and Records Administration
Joyce Pappas	Headquarters, Air Force Materiel Command
Nathan Paxton	Office of U.S. Senator Angus S. King, Jr.
Kathy Pherson	Pherson Associates LLC
John Piccone	Office of Congressman Jim Banks
Jason Pierce	Office of the Administrative Assistant, Office of the Secretary of the Air Force
John Powers	National Archives and Records Administration
Megan Reiss	Office of Senator Mitt Romney
Ricardo “Brandon” Rios	House Committee on Oversight and Reform
Harvey Rishikof	American Bar Association Standing Committee on Law and National Security
Matthew Roche	Defense Counterintelligence and Security Agency (DCSA), Critical Technology Protection Directorate

Golan Rodgers	Former House Foreign Affairs Committee's Subcommittee on the Middle East and North Africa   Former Department of State's Arms Control, Verification and Compliance Bureau
Ethan Rosenkranz	U.S. Senate Committee on the Budget
Jon Rosenwasser	Senate Select Committee on Intelligence
Mike Rutka	Information Security Branch, Office of Security, U.S. National Geospatial-Intelligence Agency
Tom Savage	Embassy of Australia, Washington DC
Gary Schmitt	American Enterprise Institute
Grant Schneider	National Security Council
Daniel Schuman	Demand Progress & Demand Progress Education Fund
Roman Schweizer	Cowen and Company, LLC
Michael Shaughnessy	U.S. Government Accountability Office
Susan Shekmar	LinQuest Contractor Support, Office of the Assistant Secretary of the Air Force for Space Acquisition and Integration
Carly Smith	Embassy of Canada, Washington, DC
Mandy Smithberger	Office of U.S. Senator Elizabeth Warren   Former Center for Defense Information, Project On Government Oversight
Alex Snider	Office of Senator Christopher Murphy
Henry Sokolski	Nonproliferation Policy Education Center
George Spencer	British Defence Staff, British Embassy
Sharon Squassoni	George Washington University
Alissa Starzak	Public Interest Declassification Board
Kelvin Stroud	Aerospace Industries Association
Bill Studeman	Retired Admiral, U.S. Navy   Former Public Interest Declassification Board
Moon Yousif Sulfab	Office of the U.S. Senate Republican Leader Mitch McConnell
Conner Swett	HillVets Fellow
Frank Tedeschi	Office of Senator Mike Rounds
Michael Thomas	Office of the Director of National Intelligence
Jason Theriault	Defense Counterintelligence and Security Agency (DCSA), Critical Technology Protection Directorate
William Tobey	Belfer Center for Science and International Affairs, Harvard University
Leonor Tomero	Office of the Undersecretary of Defense for Policy
Maria Vastola	U.S. House Armed Services Committee
Steven Vogel	Information Security Branch, Office of Security, U.S. National Geospatial-Intelligence Agency
Kenneth Wainstein	Former Public Interest Declassification Board   Davis Polk
Eric Wakin	Hoover Institution, Stanford University
Mark Webber	Lockheed Martin Corporation
Keith Webster	Defense and Aerospace Export Council, U.S. Chamber of Commerce
James Wilson	Office of the Historian, Department of State
Benjamin Wittes	The Brookings Institution
Clint Work	Korea Economic Institute of America (KEI)
Simon "Pete" Worden	Breakthrough Initiatives



*Over-classification: How Bad Is It, What's the Fix?*

Mark Zaid	Attorney, National Security Law, Mark S. Zaid, PC.
Roger Zakheim	Ronald Reagan Presidential Foundation and Institute





605 S. Buchanan St. | Arlington, VA 22204

Email: [info@npolicy.org](mailto:info@npolicy.org)

Web: [www.npolicy.org](http://www.npolicy.org)