Comments of Steven Aftergood
Director, Project on Government Secrecy
Federation of American Scientists

Before the
Public Interest Declassification Board
on
Modernizing the National Security Classification and Declassification Systems Through the Next Administration's Executive Order

December 8, 2016

Thank you to Chairman Morrison and to the Board for getting this conversation started.

Assuming that the next Administration will in fact prepare a new executive order on classification policy, I would like to propose two specific steps for consideration: (1) a new procedure for considering declassification of *properly* classified information, and (2) a new initiative to develop and test innovative information security measures.

1. A new provision for requesting declassification of "properly classified" information

I suggest modifying the current provision in Section 3.1(d) of E.O. 13526 to establish new procedures that would enable the public to seek declassification of properly classified information.

As things stand, information that is "properly classified" is exempt from the Freedom of Information Act. Likewise, mandatory declassification review does not extend to properly classified information. Classification challenges under Section 1.8 of the executive order only apply to information that is "improperly classified."

It is true that Section 3.1(d) does currently permit discretionary declassification of properly classified information by the original classifier when "questions arise" about whether the public interest outweighs the need to protect the information. But it provides no procedures for actually <u>raising</u> such questions, or for third-party review of the original classification decision.

So there is a gap in current policy with respect to the possibility of declassification of *properly* classified information.

We know that properly classified information is sometimes of such profound public interest that withholding it is undesirable and counterproductive.

That was the conclusion that was eventually reached by Director of National Intelligence James R. Clapper concerning the program to collect telephone metadata (known as the 215 program) that was revealed in 2013 by Edward Snowden. DNI Clapper determined in retrospect that early disclosure of the 215 program would have been the best move from all points of view.[1] Yet as an ongoing intelligence surveillance program, it was properly classified under the terms of the executive order, and there was no effective procedure for raising and reconsidering the question of its declassification.

Therefore, I propose that the next executive order should include a provision that would allow members of the public to initiate an appeal to an entity *other than the original classifying agency* – perhaps a new ISCAP-like body, or an enhanced PIDB with its own declassification authority – and to argue that a category of information that is currently and properly classified should nevertheless be reviewed for declassification and disclosure in light of a compelling public interest. The reviewing entity – which must be independent of the original classifier in order to provide a fresh, unbiased assessment – would be tasked to weigh that larger public interest and to render judgment about whether or not to sustain, or modify, the original classification.

What types of classified information might be subject to such procedures? Notionally, they include intelligence supporting a U.S. decision to engage in military operations, the conduct of detention and interrogation activities, the casualties arising from targeted killing operations, and other categories of information that may be squarely within the boundaries of information that is otherwise properly classified, but that are also of momentous public interest.

A process to enable deliberate declassification of such information should be incorporated in the next executive order.

2. Create a test-bed for new classification policies

Although President Obama spoke in 2009 of pursuing "a more fundamental transformation of the security classification system," such a transformation has not yet occurred. In part, that is because the current system continues to serve a basic information security function and, in part, because superior alternative approaches have not been devised, tested or validated in practice so that they could be adopted.

It is time to undertake that task of creating the "next" national security classification system.

[1] See Eli Lake, "Spy Chief: We Should've Told You We Track Your Calls," *The Daily Beast*, February 17, 2014; available at http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html

The current executive order is unlikely to be replaced all at once by an order that prescribes a wholly new and different system. Rather, new approaches may be chosen once they have been proven effective on a small scale. It will be necessary to "build a bridge" to the next classification system through trial and error.

So the next executive order should mandate the development and testing of "next-generation" classification and declassification procedures on a trial basis.

Of course, it is not enough that these procedures be new and different. They must also meet other criteria such as: simplicity, cost-effectiveness, ease of use, responsiveness to oversight, robust error correction, minimized scope and duration of control (in the case of classification), and increased productivity (in the case of declassification).

Among the kinds of measures that could be evaluated and certified for broader use are emerging technological approaches to facilitating classification and declassification, radical reductions in formal controls on information, expanded authority to declassify, traceability of classification throughout the information life cycle, increased flexibility in authorized access, and so forth.

Who should perform such development and testing? The Department of Defense, which is the largest generator of classified information, would seem to be a logical choice.

Within DoD, there is a Strategic Capabilities Office (SCO) that is tasked to pursue "disruptive applications and new and unconventional uses of existing system and near-term technologies" including "program information management strategies, objectives and technologies."[2]

While national security classification policy has not been considered part of the SCO portfolio up to now (and it may not want the job), this Office might be a good fit particularly because of its emphasis on practical innovation.

*

Thank you for considering these suggestions.

[2] DoD Directive 5105.86, Director, Strategic Capabilities Office (SCO), November 14, 2016; available at http://www.dtic.mil/whs/directives/corres/pdf/510586_dodd_2016.pdf