OPEN SOURCE SOLUTIONS, Inc.
International Public Intelligence Clearinghouse
1914 Autumn Chase Court
Falls Church, Virginia 22043-1753

Voice: (703) 536-1775 | Facsimile: (703) 536-1776
INTERNET: steeler@well.sf.ca.us

COMMENTS on
Executive Order 12356, "National Security Information"
by
Mr. Robert D. Steele, President and Owner
OPEN SOURCE SOLUTIONS, Inc.

for
Presidential Inter-Agency Task Force on National Security Information
Department of Justice, 9 June 1993

National Security Information Should NOT Be Classified "By Definition"

The most fundamental flaw of the Executive Order as written is that it equates national security information with "classified information". No where have I ever seen it written that intelligence must be classified, nor have I seen it demonstrated that information of importance to the Nation must of necessity be classified. I have in fact, in resigning from government two years short of retirement, dedicated myself to demonstrating that the opposite case is true: that the wealth and health of the Nation depend much more on a public intelligence capability, a capability to collect, process, and disseminate unclassified information.

Classification Definitions Correct But Insufficient and Ignored

The existing definitions of "Top Secret", "Secret", and "Confidential" are adequate in theory, but are rendered irrelevant because of the complete lack of Presidential direction as to how one should define "national security", "exceptionally grave damage", "serious damage", or "damage". The fact of the matter is that the agencies considered to be part of the national security apparatus have taken it upon themselves to define everything they do,

everything about them, to "be" vital to national security, and they have taken it upon themselves to classify everything about themselves, their operations, and their products, without regard to the definitions established by the President in this Executive Order.

Unclassified Information ("The Competition") Is Buried In A "Cement Overcoat" of Classified Information, Making It Unusable By The Consumer

In my experience, at least 50% of what the intelligence community does is unclassified--unclassified sources, unclassified methods, unclassified products. Unfortunately, because of the total discretion allowed to the community, all that is unclassified is buried, literally, inside of tightly controlled documents bearing the classification of the most sensitive piece of information. Many senior analysts and intelligence community managers have commented on this problem--the President's own intelligence daily frequently contains unclassified information that cannot be released to Congress or the press because it is not identified as unclassified and is contained in a classified document.

A specific example from my experience: as a resource manager at Headquarters Marine Corps, I was party to a contracted effort to review Marine Corps capabilities and limitations with respect to communications, computers, and intelligence in support of each of the theaters. Despite my direction to the contractor that the product be unclassified (I specified "For Official Use Only", we ultimately received a three-inch binder classified "Secret". Upon examination it became evident that the entire volume, with the exception of about twenty pages on "deficiencies" was unclassified. The Executive Order, Section 1.3(a)(2), is being used as the basis for obscuring fundamental information needed to mobilize support for correcting generic deficiencies.

The general categories of information eligible for classification, as set forth in Section 1.3 of the Executive Order, are good ones, but require much stricter definition and oversight.

Employees Have Not Been Trained to Exercise Discriminate Classification

It has been my experience that employees of the various intelligence community organizations routinely classify everything they collect, everything

they write. This is in part because there are severe penalties for under-classifying information, and there are no penalties for over-classification, even if over-classification is against the public interest.

Firm Limits on the Duration of Classification Urgently Needed: Two Years (Confidential), Five Years (Secret), Ten Years (Top Secret)

I believe that specific limits should be set on the duration of classification. This is the "age of information", and the laws of cybernetics rather than the laws of physics are now paramount. The "half-life" of information, even classified information, gets shorter every year. In my judgement, a new Executive Order should, in addition to providing much firmer direction on what constitutes "national security" and "damage", must also specify that with certain strictly limited and supervised exceptions, all classified information is automatically declassified when it reaches ten years of age. Confidential should be declassified after two years, Secret after five, Top Secret at between seven and ten years depending on the topic and country.

Violation of the Prohibition on the Use of Classification to Conceal Impropriety or Questionable Activities Appears Routine, Without Sanction

It appears to me that the prohibition established in the Executive Order, against the use of classification in order to conceal violations of the law, inefficiency, or administrative error, and so on, is itself violated with frequency, whether by design or by habit. The following quotation from a former member of the National Security Council is instructive:

> **"Everybody who's a real practitioner, and I'm sure you're not all naive in this regard, realizes that there are two uses to which security classification is put: the legitimate desire to protect secrets, and protection of bureaucratic turf. As a practitioner of the real world, its about 90 bureaucratic turf; 10 legitimate protection of secrets as far as I'm concerned."**

That observation was made by Rodley B. McDaniel, then Executive Secretary of the National Security Council, to a Harvard University seminar. He was quoted in Thomas P. Croakley (ed), *C3I: Issues of Command and Control* (National Defense University, 1991), on page 68, and again in my

own "C4I Campaign Plan: Proposed Changes in How We Do Business" (C4I Department, Headquarters U.S. Marine Corps, 16 July 1992), page 8.

As an initial remedy against over-classification, I would recommend three measures:

First, integration of training on the revised Executive Order and the intent of the President regarding classification, into the training program of all government employees and their industry counterparts. The training model established in relation to Executive Order 12333 stands as proof that reaching individual employees can make a difference.

Second, elimination of "delegated" authority. In my experience, employees at the very lowest levels of the intelligence community routinely classify documents, and are given the identify number of the person in their chain of command who does have delegated authority to classify documents. They type that is just as if the person had seen the document and approved its classification. Instead, in conjunction with the training program, we need to make the originator of the document, however junior, accountable for its classification.

Third, a much stronger program of oversight, beginning with a complete review of all intelligence production including the daily current intelligence products provided to the President and his senior staff. Measures should be adopted with prevent unclassified information from inheriting the classification of companion information which is legitimately classified, and sanctions should be imposed on organizations which persist in this practice.

Routine Declassification Simply Does Not Happen

Although the existing Executive Order calls in Section 3.1 for the declassification or downgrading of information as soon as national security considerations permit, this provision is, in my experience, ignored in its entirety within the national intelligence community. All documents are classified for the maximum period possible, and all documents which can be exempted from automatic declassification are exempted. This is not done for malicious reasons--it is done for bureaucratic convenience, for it is far easier to "play safe" and have one (maximum) standard, than to train and support employees in applying discretionary judgement.

Intelligence Security Oversight Office Has No Teeth, Has Been Ineffective

I have never, in eighteen years of experience, encountered a representative of the Intelligence Security Oversight Office, or heard of a spot check of any documents associated with any office I have ever been associated with. Although Section 5.2 provides the Office with the authority to conduct on-sight inspections, this does not appear to be a common practice.

In my experience, the Information Security Oversight Office has been a "zero", irrelevant and ineffective. It needs teeth--a staff, and the authority to spot check. It should pay particular care to the over-classification of information which was unclassified to begin with, but which was classified to justify a report by an intelligence agency (instead of turning it over to another government agency), to "protect" the collection agent (whose identify could easily have been obscured or deleted), or which has been buried by attaching relatively minor but more classified material to it.

Across the Board Evaluation Required: Need to Focus on Existing Unclassified Sources, Methods, and Products, Prevent Their Being "Buried" by Classified

I strongly recommend an across the board evaluation of intelligence community collection, external research and analysis, and production, to determine the percentage of sources, contracts, and products which are inherently unclassified, but whose value is being lost because of the excessive classification environment in which the unclassified information is being exploited. In my view, any document which is comprised of 50% or more of unclassified materials, should be split in to an unclassified primary document with a classified appendix.

No Exemptions to Access Regulations Should be Permitted

I find the exemption of the President and his staff from the provisions of Section 3.4(a) to be offensive and contrary to democratic principles. The President and his staff should have the same authority to classify information as the national security agencies, but they should not be exempted from declassification review.

Section 4.3 has no rational foundation. Historical researchers should be satisfied by an Executive Order which radically increased the amount and pace

of declassified documents available for public examination. Former Presidential appointees should be held to the same standard as former government employees. If they retain their security clearances and have a need for access, they should be granted access. If they do not retain their clearances, they should not be granted access.

I have the impression that security has been remarkably lax on the many occasions when political appointees have resigned and left their offices with boxes of classified documents. This is intolerable.

Special Access Programs Abused, Source of Enormous Waste of Dollars

The intelligence community has also seriously abused its prerogative, established in this Executive Order, to create special access programs. It has been my experience that special access program lead to enormous waste because they prevent the sharing of normal capabilities and information.

By way of example, I will note that I have met with a number of contractors, each employed under a different special access program, and each charged with creating the ultimate all source fusion workstation. I believe the waste in redundant research & development for information handling by special access programs to be on the order of $100 million a year.

Section 4.2, permitting the establishment of Special Access Programs by agency heads, should be revised. Agency heads should be permitted to recommend the establishment of such programs, but a single office responsive to the President, such as the Information Security Oversight Office, should be the sole approved authority, and should establish strict "sunshine" provisions.

It is my understanding that the Special Access Programs result in enormous waste in that contractors are required to keep selected employees, documents, and equipment completely isolated, to the point of building separate vaults for them, and are then also subject to the sometimes arbitrary and sometimes capricious dictates of whoever is administering "security" for a Special Access Program. Any future Executive Order, if it permits Special Access Programs, should establish guidelines which prevent agencies from imposing unreasonable demands on contractors.

Fundamental Premise of the Order Must be Changed:
Information is Most Useful to the Nation When Widely Disseminated,
Should Not be Classified Without Cause

As a final comment, I would state my belief that any Executive Order promulgated in the future should begin with the premise that information, including intelligence, is most useful when widely disseminated, and that information must be considered unclassified until a solid case for its classification can be established. That is not the practice today.

Open Source Intelligence: STRATEGY Proceedings, 1997 Volume III 6 th International Conference & Exhibit Global Security & Global - Link Page

Previous	PART I. SECRECY & OPENNESS: TESTIMONY of Mr. Robert D. Steele, President & Owner OPEN SOURCE SOLUTIONS, Inc. to Presidential Inter-Agency Task Force on National Security Information Department of Justice, 9 June 1993
Next	PART I. SECRECY & OPENNESS: E3i-Ethics, Ecology, Evolution and Intelligence

Return to Electronic Index Page