DYSFUNCTIONAL
Information Restrictions

M. E. Bowman

It was no surprise when the 9/11 Commission reported that the government keeps too many secrets – in fact, it was not even a particularly astute observation. That criticism has been voiced many times – by privacy interests, by Congress and even by multiple administrations of the Executive Branch. Assuming that criticism is a fact, the question remains why it might be so. When the late Senator Daniel Patrick Moynihan headed a commission on secrecy in 1997, he found that an Executive Order of President Clinton assigned original classification authority to 20 federal officials, but that the power to classify even at the "Top Secret" level had spread to more than 1,300 original classifiers. The implication apparently intended was that too many people had the power to classify, creating a problem of over-classification.[1]

Others who look at the issue, usually from the outside, consider that the power to classify equates to the ability to protect turf and power. It would not take a great deal of research, or oral history, to demonstrate the poignancy of truth of these, and similar views. However, the passage of time and the regularization of procedure has, for the most part, relegated both views to the province of folklore with only vestiges of the "bad old days" still remaining. Those allegations may have been true at a point in time, or at many points in time, but any realistic appraisal of classification today will lead the researcher to a logical conclusion that both over-classification and over-long duration of classification are culturally governed by a decades-old process of protecting government information – a process that exudes an aura of reverence for the underlying theory behind them – a process that has become dysfunctional in the face of current needs of national security.

While the criticism of the 9/11 Commission was no surprise, it should be a concern that so little has been done in the past several decades to address an issue recognized by so many for so long. Perhaps of even greater concern is that so little has been accomplished since that report, even though both the President and Congress have expressly mandated policy changes to facilitate sharing of information within the Government, with state, local and tribal officials and with foreign powers. These mandates beg the question – if will power doesn't achieve the result, are the underlying policies by which we restrict the availability of information the ones we need today? Put another way, have the venerable policies of protecting sensitive information created a culture of restriction resistant to change?

The answers lie in the rationale for restricting the availability of information. A great deal of information restriction is legacy, stemming from the felt need to guard military-related information from disclosure to those who can harm us. A more limited quantity of information may be restricted in the interests of efficiency of government. To accommodate that interest, the Congress, in enacting the Freedom of Information Act,[2] permitted exemption from mandatory disclosure of pre-decisional advice to decision-makers, data relevant to criminal investigations and information of so minor a nature as to not merit the effort to retrieve and disclose it. Other data has been predetermined by Congress to merit withholding. This might include nuclear energy-related information, information about the personnel and processes of intelligence organizations or personal privacy information.

However, classified information is not the only problem of information restriction. Some data becomes restricted, as a practical matter, by virtue of a label. One of the most vexing issues concerning the availability of government information has been a proliferation of undefined caveats intended to describe, and channel, unclassified information. These include "for official use only," "sensitive but unclassified," "sensitive homeland security information," and "law enforcement sensitive," among others. For ease of discussion, these will be collectively referred to as Controlled Unclassified Information (CUI). While many Government agencies may use CUI, and any number of CUI caveats, there is generally no standard definition for them – nor is there a common standard by which the underlying data is intended to be protected. Most problematic, there is no efficient method of determining who is eligible to receive information annotated with those caveats (often a greater problem for initial recipients of the data than for the originators). Steve Aftergood of the Federation of American Scientists believes this proliferation to be a bigger problem than over-classification.

Finally, whatever the purpose of creating CUI caveats, it has become clear since 9/11 that many of them have evolved with a subtle whimsy to encompass elements of information and control that serve to protect national security - elements that deal, for example, with terrorism, international narcotics trafficking or details of foreign policy. For those who witnessed the development of these

1. Although classification by individuals was the norm in eras past, today the preference is to classify by a classification guide and to use Original Classification Authorities for declassification. The existence of a standard for classification is a milestone on the road to rational protection of information.

2. U.S. Code § 552

CUI caveats as vehicles to serve limited, agency-specific needs, this evolution will be puzzling, but it is a fact vital to understanding and resolving contemporary needs. To continue, it is a worthwhile exercise to re-examine the concept of "national security information."

NATIONAL SECURITY INFORMATION

Of course, we know what national security information is because it is defined in Executive Order 13292 as classified information relating to the national defense or foreign relations, the disclosure of which could reasonably be expected to cause damage to national security. That definition is the first of several dysfunctional legacy concepts of national security that leads, in this article, to an heretical proposition – information recognized as vital to the well-being of the nation and its people need not, and should not, rely on principles of classification. A second, but closely related heresy is that traditional notions of national defense and foreign policy are concepts that, in the post 9/11 world, are far too narrow to define the information relevant to the security of the nation today. To evaluate these issues, it is necessary to look first at the standards for both classification of information and the standards for access to it.

CLASSIFICATION

Any analysis of information restriction by the Government, as restrictions are practiced today, has to begin with classification, and any analysis of classification begins with military purpose. More than two thousand years ago Sun Tzu, in his classic, ***The Art of War***, wrote "the formation and procedure used by the military should not be divulged beforehand." A fast-forward to the American Revolution illustrates that American classification began in a prelude to war when the First Continental Congress, on September 6, 1774 passed the following resolution:

> *Resolved that the doors be kept shut during the time of business, and that the members consider themselves under the strongest obligations of honor, to keep the proceedings secret, until the majority shall direct them to be made public.*

In peace, the practice continued as President George Washington transmitted "confidential communications" to Congress. However, it was not until 1869 that the first official classification schematic was issued. In that year, the Army issued an order restricting the availability of information on Army fortifications. From that point until 1940 all classification determinations were made in accord with military directives.

The modern era of classification begins with President Franklin D. Roosevelt who issued a very rudimentary Executive Order, 8381, as the first Executive Order dealing with classification. The reasons for this Order are somewhat obscure, but two factors certainly seem relevant. First, by 1940 the defense establishment had grown substantially to include a large civilian work force. Since the principle of civilian control is an article of faith in our system, it would be logical to give civilians the ability to make classification decisions rather than leave all such decisions to their military subordinates. Second was the Manhattan Project. Although the scientists working on the Project agreed to forgo their standard practice of collaboration with others, and to maintain a voluntary censorship, it was necessary to provide guidance to government employees as well. For this, a military directive was ineffective.

Executive Order 8381 was simplistic in form and substance. Essentially, this Order permitted classification of all information pertaining to the military, its facilities or military plans. Classifications were Secret, Confidential and Restricted. This was followed by two classification Orders issued by President Truman. The first, EO 10104, issued February 1, 1950, essentially continued the Roosevelt Order, adding Top Secret as a category. The second, EO 10290, issued September 24, 1951, permitted non-military agencies to classify, thereby expanding the universe of potentially classified information. It is probably worth remembering, at this point, that Americans have a natural antipathy for secrecy, and that antipathy came through even in this immediate post-war climate. Although EO 10290 specified that information should be protected at the lowest level consistent with the national security, the Order was quickly attacked by Congress and the press as being overly permissive. Put more simply, it was viewed as a document that too easily kept information from the public.

President Eisenhower, perhaps taking a lesson from the reaction to the second Truman Order, issued his own Order, eliminating the Restricted category, reducing the number of agencies that could classify and mandating professional managers for classification, as well as training and orientations programs.[3] He also provided for downgrading, declassification when warranted and adopted a truly radical concept – automatic declassification on a date certain.[4] President Kennedy maintained most of the Eisenhower provisions, but also established four categories of information, one which would require automatic declassification in twelve years, one which would be downgraded at three-year intervals until declassified and two which would be exempt from declassification.[5]

President Nixon broke new ground with his Order on classification. In many ways, it was as sweeping a reform as

3. Although the attempt to eliminate capricious classification and security practices with regularized process cannot be faulted, as explained herein, even the most salutary intent can have unintended consequences. In this case, one consequence of the mandatory training that grew from this Order may have been a cultural resistance to change.
4. Executive Order 10501, issued December 15, 1953.
5. Executive Order 10964, issued September 20, 1961.

had been the Eisenhower document. Reflecting the mood of the public, Nixon issued 11652 on March 8, 1972 with the statement that

> *"Unfortunately, the system of classification which has evolved in the United States has failed to meet the standards of an open and democratic society, allowing too many papers to be classified for too long a time. The controls which have been imposed on classification authority have proved unworkable, and classification has frequently served to conceal bureaucratic mistakes or to prevent embarrassment to officials and administrations."*[6]

This brief history of Executive Orders on classification has a purpose. First, it is important to note that this has been an evolutionary, not a static, process. More importantly, what each of these Executive Orders had in common was their devotion to things military. Each was predicated on Sun Tzu's wisdom – deny military information to the enemy or to those who, on gaining military information, could do harm to the national security of the United States. Despite President Nixon's bone to the access community, his Executive Order maintained the military flavor of his predecessors and concentrated on procedural modifications such as portion marking documents, automatic declassification time tables and mandatory review of classified information.

If we fast-forward one more time to the post-9/11 era, we find that, with the exception of procedural matters designed to provide oversight to the classification system,[7] to reduce potential classification categories and to solidify the requirement for automatic declassification,[8] little has changed from the fundamental concept that classification is intended to deny disclosure of information.[9] Much of the classification schematic is related to military matters so the concept of denial is both natural and time honored. Moreover, the training and orientation programs initiated by President Eisenhower and maintained over the past half century have made withholding of information far more a part of our culture than is the current attempt to ensure appropriate and necessary disclosures.

The question we all must consider is whether, in the modern era, the security of our nation and its people remain protected by this schematic. In turn, that depends on whether the national security means the same thing today as it did in 1940 – a subject to which we will return after considering who has access to restricted information and the lessons of 9/11. For now, we can think about the following proposition: in conflict against foreign armies, revealing information was dangerous – in conflict against terrorism, revealing information may still be dangerous, but keeping information in secure stove pipes may be even more dangerous. Regardless of anything else, the threats to the nation are different today. In a bygone era, security was the responsibility of federal employees (and federal contractors). Today, security must be the responsibility of federal, state, local and tribal authorities, and even of private industry. That alone demands a re-examination of our security paradigm.

ACCESS STANDARDS

Although the original classification Order of President Roosevelt did not regulate who in government service could classify qualifying information or have access to it, it was not long before the more restrictive and evolving notion of "need to know" developed. Nearly every person who reads this article will have lived under this principle. Succinctly, it means that a person may not have access unless he/she occupies a position with a "need" for classified information. Information not relevant to that position is reserved for others in different positions. Clearly, this is a logical process, but equally clearly this is a procedure of exclusion, not inclusion, and every relevant judicial test has confirmed that. Additionally, the concept of national security occupies part of the access standards. While a person's right to pursue a particular profession is within his "liberty" and "property" interests protected by the Fifth Amendment,[10] the scope of due process review is lessened when national security interests are involved.[11] The consequence is that there will be persons who will be held ineligible for some forms of federal employment because they cannot have access to classified information.

The demands of war also generated a need to be assured that those who had access to classified information were trustworthy. Our history, and that of every nation, is replete with examples of vital national security information falling into the wrong hands. Therefore, Executive Orders complementing classification standards have provided the standards by which an individual may be "cleared" to receive classified information. Those not "cleared" are excluded from access to classified information. In fact,

6. Executive Order 11652, issued March 8, 1972, effective June 1, 1972.
7. President Carter, with Executive Order 11605, required that Confidential information be subject to an "identifiable damage" test and established the Information Security Oversight Office to monitor compliance with EO 12065.
8. President Clinton, on April 16, 1995 issued Executive Order 12958.
9. President Bush maintained all the provisions of the Clinton Order, adding Weapons of Mass Destruction as a category of information subject to classification. Executive Order 13292 issued March 25, 2003. The categories of information subject to classification are: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the United States, including confidential sources; (e) scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism; (f) United States Government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plan, or protection services relating to the national security, which included defense against transnational terrorism; or (h) weapons of mass destruction.
10. Green v. McElroy, 360 U.S. 474 (195).
11. Department of the Navy v. Egan, 484 U.S. 518 (1988).

Congress has made certain employment decisions completely unreviewable if based on national security.[12]

ACCESS LESSONS OF 9/11

Many lessons can be drawn from the 9/11 terrorist attacks, but one that appears to be universally accepted is that the government does not manage its information well. In particular, information in the possession of the federal government frequently is dysfunctionally stovepiped and/or jealously guarded. That point is not worth belaboring, but it is worth considering why it may be true. Again, the issues revolve around classification and caveat - leaving ample room, of course, for the possessory instincts of agency employees who have worked hard to accumulate information.

As noted previously, caveated CUI results in a practical form of information exclusion, even within the federal government. Classified information, by contrast, is specifically designed for exclusion. Executive Order 12968 sets the current standard for access to classified information, and it takes little reflection to understand that it, like all its predecessor Orders, is also designed for exclusion. For example, the Order contemplates access only by federal employees and federal contractors, only on a demonstrated need-to-know basis and only by as few individuals as can meet the needs of an agency.

Sec. 1.2. Access to Classified Information.

(a) No employee shall be granted access to classified information unless that employee has been determined to be eligible in accordance with this order and to possess a need-to-know.

(d) All employees shall be subject to investigation by an appropriate government authority prior to being granted access to classified information and at any time during the period of access to ascertain whether they continue to meet the requirements for access.

Sec. 2.1. Eligibility Determinations.

(b) The number of employees that each agency determines are eligible for access to classified information shall be kept to the minimum required for the conduct of agency functions.

(b) (2) access to classified information shall only be... granted based on a demonstrated, foreseeable need for access.

Sec. 2.5. Specific Access Requirement.

(a) Employees who have been determined to be eligible for access to classified information shall be given access to classified information only where there is a need-to-know that information.[13]

Although not nearly so formal a process, a similar result obtains for CUI. The principle of this form of control is to channel the information to those who use it. The practical consequence of these "channels" is to restrict access by those outside processes which the channel is intended to serve. CUI may be more permissively available within government, but even there, the information generally travels only within the scope of the employment of relevant actors. With exceptions related to the purpose of the channel, it is a specific exclusionary concept for those outside of government and a practical exclusion for most within government.

What makes CUI especially difficult to deal with is lack of standards. Not only is most of it undefined, or defined differently by different agencies, a government contractor who receives "for official use only (FOUO)" information from government agency "A" may be required to store that information in a locked filing cabinet, but need only place similarly marked information from government agency "B" in a closed desk drawer. Government agency "C" may expressly prohibit transmittal of FOUO information over the Internet while government agency "D" may permit it simply by not addressing the issue. Moreover, neither classified information nor CUI were designed with processes for disclosure to persons not working on behalf of the Government – which brings us to 9/11.

A necessary question, heretical even to suggest, is whether this access paradigm can continue in the face of current transnational threats. These standards, a limitation to employees, strict need to know, mandatory background investigations and minimum numbers with access, become critically important in the current climate of terrorism. The nineteen hijackers of 9/11 lived in the United States, had credit cards, bank accounts, telephones, automobiles and flew frequently on commercial airlines. They had encounters with police, ticket agents, motels, restaurants and even prostitutes. They lived as do millions of others in the United States, behaving normally and attracting little attention. Neither intelligence agents nor FBI were likely to stumble across these men. In fact, if anyone were to encounter them in a way that might be remembered, it most likely would have been one of the seven-hundred fifty-thousand state,

Whenever you have an efficient government you have a dictatorship.

— Harry S. Truman (1884 - 1972), Lecture at Columbia University, 28 April 1959

12. E.g., in Carlucci v. Doe, 109 S.Ct. 407 (1988), the U.S. Supreme Court held that NSA may remove an employee pursuant to 50 U.S.C. section 831-32 without adherence to the suspension and hearing provisions of 5 U.S.C. section 7532.
13. See, e.g., Webster v. Doe, 486 U.S. 592 (1988).

local or tribal police.

Moreover, many of the threats to the Homeland revolve around symbols. Bridges, buildings, monuments or shopping centers are among the "targets" of terrorism. For the most part, these are rarely federally protected, which means that when there is a threat to one of these, and we have seen many in the past few years, local officials, to include governors, mayors, police, fire and national guard must have information that is generally available only to federal officials, and, under current procedures, available only under the conditions relevant to the type of information held.

SHARING REQUIREMENTS

To meet the obvious concern, the Commission recommended both Presidential and Congressional mandates for sharing of information while protecting privacy. Following the Commission's findings, President Bush presaged the coming Intelligence Reform and Preventional of Terrorism Act with Homeland Security Presidential Directive Six (HSPD-6) on September 16,2003, and Executive Order 13356 on August 27, 2004. These mandated a sea change in the way the intelligence community does business. E.O. 13356 directed the Intelligence Community to:

> *give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information;*

Among the innovations of that Order was the direction for agencies to "write to release," requiring:

> *at the outset of the intelligence collection and analysis process, the creation of records and reporting, for both raw and processed information... in such a manner that sources and methods are protected so that the information can be distributed at lower classification levels, and by creating unclassified versions for distribution whenever possible;*
>
> and by
>
> *requiring records and reports related to terrorism information to be produced with multiple versions at an unclassified level and at varying levels of classification*

The object was to instill an information sharing environment so that all relevant information could be brought together. In furtherance of that goal, originator controls were discouraged. The most significant act of the President, however, was to define the sharers. HSPD-6 provides that:

> *[I]t is the policy of the United States to (1) develop, integrate, and maintain thorough, accurate, and current information about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism (Terrorist Information); and (2) use that information as appropriate and to the full extent permitted by law to support (a) Federal, State, local, territorial, tribal, foreign-government, and private-sector screening processes, and (b) diplomatic, military, intelligence, law enforcement, immigration, visa, and protective processes.*

Of more than passing interest is the sequence of the wording in that paragraph. Priority was given to those who might more likely come in contact with the individual terrorist. The reason for that stems from lessons learned, recounted above, of the nineteen hijackers and the many public contacts they had while living in the United States. The simple fact is that there are literally millions of Americans, without clearance, who have a "need to know" some information that, traditionally has been held within the exclusive province of the relevant Executive Branch employee.

To round out this effort, the President also directed an outreach program to acquire intelligence on terrorism that might not be available through United States mechanisms. HSPD-6 directed the Department of State to seek information from other nations.

> *The Secretary of State shall develop a proposal for my approval for enhancing cooperation with certain foreign governments, beginning with those countries for which the United States has waived visa requirements, to establish appropriate access to terrorism screening information of the participating governments.*

The "need-to-share" mantra has been chanted by all. It is found in academic analysis, political articles, Executive Branch directions and Congressional statute. An entirely new concept was identified by Congress and endorsed by the President when Congress directed that an "Information Sharing Environment" (ISE) be created.[14] No one doubts the need. As Admiral Jacoby, when Director of the Defense Intelligence Agency stated that anyone who can make sense of raw data, and those who are the consumers of intelligence, are the rightful proprietors of information, not the organizations which collected it. FBI Director Mueller similarly noted that the value of intelligence is best judged by its user, not its producer. The goal...is to put the right information in the hands of the decision-makers, whether that person is in the oval office, on the battle field or patrol-

14. The Intelligence Reform and Terrorism Protection Act states that "The President shall—(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." Intelligence Reform and Terrorism Prevention Act of 2004, PL 108-408 §§ 7211-7214,. 118 Stat. 3638, 3825-3832 (2004).

ling the nation's streets.

Yet, the attempt to satisfy this need, unintentionally, and perhaps largely unknown, is being hampered by the obstacle of procedures that are time-honored and useful for their intended purpose, but which were designed to deny widespread dissemination of official information. The practical effect of this represents a sharing problem whether the information is classified or unclassified but controlled. Additionally, those procedures hold within them the legacy instinct to classify information, and to retain it in classified form. Why? Because we've always done it that way, because that legacy did serve to protect the nation in a different era, and because, after the Eisenhower Administration, we have always trained to do it that way. For those of us old enough to remember the legacy of the Cold War, it is a truism that no one ever got in trouble for over-classifying, or, indeed, merely for keeping one's mouth shut. Indeed, revealing "too much" generally has been considered career-threatening. It was for that reason that Congress has consistently sought means to protect whistle-blowers, but even legislative protection cannot guarantee a soft-landing when a person takes an unpopular course of action and reveals more than superiors believe to be proper.

We cannot afford today to cling to concepts that were meant to meet exigencies of a bygone era. To be sure, much information still requires tight protection. War plans and weapons systems are the obvious targets for protection, but vulnerabilities of infrastructure, intelligence sources and methods and the recipes and blueprints for Weapons of Mass Destruction still require protection. As well, data such as proprietary information of industry requires government assistance to secure data that is critical to the economic health of the nation. However, it is clear that the primary threats to the nation today revolve around individuals, not nations. Put simply, that means that any scheme that does not put information in the hands of those who can best use it, i.e., those who come in contact with individuals, creates a threat to our society.

The fundamental mantra has changed. In a bygone era, "when in doubt, classify" was the accepted, perhaps even demanded, practice. Today there is an impetus to "share." However, we must take exceptional care not to let the pendulum swing too wide. If the mantra becomes "when in doubt, share," we could find that we have created a paradigm even more dangerous than the old one. "When in doubt, ask" should be the preferred practice.

The problem is more than one created by Executive fiat or practice. What President Roosevelt did in 1940 is not dissimilar to what President Bush did in 2003. Both, and all the presidents in between, provided guidance for Executive Branch employees and contractors, and created mechanisms that bound those employees to objectively sustainable standards of conduct. These were not illogical measures, but to meet current exigencies, and to remediate the culture that springs from those measures, requires substantial effort to modify decades of legacy philosophy.

First, the proliferation of CUI caveats should be brought under control. Second, those caveats used must have common definitions and common standards of control. Third, the classification and access Executive Orders should be re-written to reflect the need to disseminate, not merely the need to withhold. Fourth, and far more problematic, all this has to be made applicable to the non-federal employee or contractor. That alone requires legislation that applies to all persons the philosophy and the standards of access required to meet contemporary threats.

Obviously, this represents a herculean task – one that is far more difficult to administer than are the current, and far more comfortable scheme(s). There is, however, a template from which to consider a way forward. The classification schemes begun by President Roosevelt and carried forward to the present day did have one point of departure. As a direct result of the Manhattan Project, and recognition of the awesome power of nuclear weaponry, the United States classification scheme split in 1946.

The Atomic Energy Act of 1946 was enacted to control technological data related to nuclear weaponry. More than that, it removed classification from the near exclusive province of the Department of Defense (DOD). All control of nuclear energy was transferred from DOD to the civilian Atomic Energy Commission (AEC). The rigid controls of the Manhattan Project were maintained, but by statute rather than Executive Order in order to broaden the controls and make them applicable at large, rather than solely to the Executive Branch.

A new category of information, Restricted Data (RD), was created to define the limited scope of the statute:

> *"...all data concerning the manufacture or utilization of atomic weapons, the production of fissionable material, or the use of fissionable material in the production of power, but shall not include any data which the commission from time to time determines may be published without adversely affecting the common defense and security."*[15]

Subsequently, in 1954, the Department of Defense successfully lobbied Congress to relax control over RD. RD was intended to protect nuclear weapon design, manufacturing processes and effects, but it proved a bit too restrictive because the military establishment still had a need for some such access and an additional need for access regarding nuclear weapons deployments. Taking a chapter from King Solomon, Congress maintained the stringent controls over RD, but established one more new category of information – Formerly Restricted Data (FRD). The Atomic Energy Act (as amended) now permitted removal of some RD data to FRD status and gave DOD access to that data under DOD clearances. RD clearance, termed a "Q" clearance, is managed by the Department of Energy, FRD is an access indicator for those with a need-to-know and possessing an appropriate clearance authorized by the by the Department

15. Atomic Energy Act of 1946, PL 585 § 10(b)(1) codified originally at 42 U.S. Code, §§ 1801 et seq.

of Defense. This change permitted selected atomic energy information to become more accessible to the DOD and to some United States industry, as well as to certain of the international community.[16]

Information which fit the definition of RD was deemed to be "born classified," meaning that it needed no classifying authority to protect it from disclosure. FRD was defined as:

> *"Classified information which has been removed from the Restricted Data category after DOE and DOD have jointly determined that it relates primarily to the military utilization of atomic weapons, and can be adequately safeguarded in the same manner as National Security Information."*[17]

Additionally, changes made in the Act now permitted the intelligence community (IC) to discuss acquired RD with the source of the information, even if the source was foreign:

> *"Classified information concerning atomic energy programs of other nations which has been removed from the Restricted Data category after DOE and the Director of Central Intelligence (DCI) have jointly determined that it can be adequately safeguarded as defense information."*[18]

Two lessons can be drawn from this experience. First, and most important, the need to safeguard sensitive data on a broader level than can be afforded by Executive Order resulted in Congress enacting legislation applicable to everyone. Second, and nearly as important is the realization that the stringent measures envisaged by the 1946 Act could be relaxed and sensitive data could be safeguarded through alternative procedures. To apply these lessons to contemporary requirements requires addressing four primary issues. First is the concept of national security. Second is the requirement for legislation that can promote a common standard of responsibility for national security information. Third is Executive Branch control of CUI and their definitions and standards for control. Fourth is a rewrite of classification and access standards that meet the cultural needs of the national security. As problematic as each of these may be, they are made exponentially more difficult by the fact that there can be no such thing as partial success. Moreover, success will be dependent on a sea change in philosophy that, in turn, rests on a realignment of philosophies relevant to the security of the nation.

NATIONAL SECURITY

Long gone is the era when definition of the threats to the security of the nation could be restricted to classified information relating to the national defense or foreign relations. Today, the information reported by a human source concerning drug trafficking or organized crime may be far more sensitive than information which, under the Executive Order, merits classification. Furthermore, it takes no imagination whatsoever to realize that the world is interdependent, nor that organized crime and public corruption are greater threats to the stability of many nations of the world than is war. It has also become abundantly clear that national economic health depends on American industry which has become increasingly vulnerable to industrial espionage. Adding to the complexities of modern life, in many areas of the world environmental problems – from wasting resources, to changing weather patterns to unlawful disposal of wastes – are cancers that eat at national viability. Moreover, national interests increasingly are seen to be concerned with the individual as much as with the broader contours of international intercourse. International norms, more and more, are beginning to confirm rights of personal privacy and the responsibility of nations to protect individuals. A quick tour of international treaties of the past few decades reveals a heavy emphasis on protection of the individual, not merely agreements regulating how they intend to interact with each other.

Simply put, the security of the nation can no longer be defined by concepts that fall exclusively within the management responsibilities of the Executive Branch. To accommodate the world as it exists, we need to understand that providing security for individuals is a multi-faceted requirement that has expanded well beyond Westphalian guarantees of territorial sovereignty. However, understanding is not accomplishing. Even in the face of a burgeoning terrorist threat, we find it difficult to exchange terrorism-related information with other nations because of enhanced, and often incompatible, concepts of privacy.[19] The problems are legion. In the United States, fingerprints are evidence but in some nations they are guarded within privacy standards. Privacy laws of the United States and those of the European Union have similar goals, but dissimilar requirements. The president may be able to direct military forces, but he cannot criminalize activities of organized crime. The legislative branch is necessary to provide incentives for education and career paths necessary to the nation's security. Some nations use their intelligence services to promote industry, making it more difficult to enforce import-export laws, patents and similar laws intended to protect and promote private enterprise.

But there is more. In 2004, an Asian tsunami, and in 2005, Hurricane Katrina taught the lesson well that natural disaster can be a matter of national security. Subsequently, in 2006, an earthquake in Pakistan and a mudslide in the Philippines confirmed the fragile grounds

16. NATO, for example has access to a certain body of nuclear weapons information subject to NATO clearance procedures. For that purpose, ATOMAL clearance is required.
17. Atomic Energy Act of 1954, as amended, §142d.
18. See, 42 U.S. Code, §§ 2153 and 2162.
19. There are, of course, practical barriers as well, including the lack of digitized files, incompatible file systems, poor centralization of records, etc. Few nations have the capabilities of the United States with respect to data storage or data manipulation.

on which national stability can rest. Events such as these overwhelm government response capabilities and undermine faith in government. Organized crime threatens both political stability of governments and the viability of international economic systems on which we all depend. Genetic enhancements to agriculture are almost certainly a requirement for the future of some, if not all nations, but it is an experimental industry that needs "adult" supervision.[20] More recently, the threat of Avian Flu has sparked widespread concern for the possibility of a global pandemic that, at its worst, could significantly destabilize world order. Then too, in an age of dramatic and accelerating technological revolution, even education may be justly considered a matter affecting the security of the nation.

To accommodate these enhanced concerns for individual and national security, we need to free our thought processes from the more traditional concepts of national security. Instead, we need to add to these thought processes the still inchoate ones that accompanied the Congressional and Executive Branch move toward a concept of Homeland Security. It is not necessary to disturb the concepts of national security, where the Executive enjoys primacy, but it is necessary to require that Congress provide additional tools, and guidance, that will partner Legislature and Executive in managing those other areas of concern that have become vital to protecting the nation.

Today we face a spectrum of problems, from terrorism to education, and each of these unique disciplines provides nearly unbounded uncertainty. Even when the consequences are clear-cut, the trade-off in values – security vs. privacy, convenience vs. economy, federal vs. local – weigh heavily on decisions. Communicating risk and solutions to the public also are crucial. Fundamentally, we have to translate information and experience into useful policy. Have we learned ways of putting all the information needed to make good decisions? If we have, can we find a way to enable what we have learned?

THE ROLE OF CONGRESS

Congress has a truly unenviable task. To enable sharing of information, and to accommodate new concepts of security, legislative initiatives are required. This will be extraordinarily difficult for two reasons. First, legislation tends to be inflexible and difficult to modify. It will not be as simple as defining Restricted Data or Formerly Restricted data. Second, legislation cannot be simplistically straightforward to be effective. Congress must provide standards applicable to all, as it did in the Atomic Energy Act, but it must also yield to the Executive substantial authority in defining terms and standards. If we have learned nothing else, it must be that the needs of national security are a moving target. Today those needs are generated by advances in technology, an eruption in organized crime and a terrorism jihadist movement that is both international and undefined.

With that as a backdrop, the work of Congress would have to support the cultural change that would come from Executive promulgations of new Executive Orders, new definitions, new standards of protection and new training mechanisms. The President can bind Executive Branch employees and contractors, but Congress must provide the authority for the public at large. As necessary, Congress will also have to provide any necessary authority to "trump" state legislation such as state laws on information disclosure.

Finally, the Congress must establish a regulatory framework that accounts for inappropriate disclosures of national security information that is both more precise and less draconian than reliance on the so-called espionage statutes alone. Disclosure remedies have vexed the nation for years past and undoubtedly will continue to do so for years to come. The magnitude of this legislative task really cannot be underestimated.

CONTROLLED, UNCLASSIFIED INFORMATION (CUI) RESTRICTIONS

As indicated above, unclassified restrictions will be an issue that must include both Executive and Legislative initiative. However, the leading edge of this problem must rest solely on the shoulders of the President. The proliferation of unclassified caveats, which result in practical restriction, of data is an enormous problem. Caveats in common use by multiple agencies, for example, Law Enforcement Sensitive (LES), have no common definitions and dissemination controls are lacking. Police are often unsure whether LES information can be disseminated to firemen, doctors or even the mayor. The Bush administration, to its credit, has recognized this as a problem and has called for an inventory of all unclassified caveats in use by federal agencies. That is a good first step.

The desirable next step is to eliminate as many as possible and then to regulate all caveats left standing.[21] One mechanism may be to start where the Freedom of Information Act (FOIA) left us in 1976. At the birth of the FOIA, "For Official Use Only" was commonly used as an anemic form of classification. After the FOIA, it was legally useful as a device indicating restricted information only if that information was otherwise exempt from mandatory

20. There have been reports of genetic engineering that, unchecked might have destroyed an entire fish population. Another experiment reportedly created a fungus that, released into the environment, might have destroyed all the vegetation on a continent. See, "Imitation of Life," Gourmet, April, 2005, pg 70.

21. Although it is desirable to reduce the number of controlled, unclassified caveats, it is not absolutely necessary. What is absolutely necessary is that they be defined, with control mechanisms clearly explained and that any such caveat in use between two or more agencies be commonly defined and utilized.

disclosure under the FOIA. It was, and remains, the "granddaddy" of unclassified caveats and could easily be used as an umbrella for all others.

We could begin with a starting point that only that information which is exempt from mandatory disclosure under FOIA may be brought with the control system of CUI and marked FOUO (or any other restrictive marking). From there, a limited number of subsets could be established for specific categories of information (e.g., LES for law enforcement data that, if exposed, could frustrate an investigation). Each category would be defined, would have established measures of protection required and would have disclosure conditions applicable to all who receive it.

CLASSIFICATION AND ACCESS STANDARDS

Finally, when the field of requirements becomes clearer, it would be time for a complete re-write of both classification and access Executive Orders, to be buttressed by any required legislation, and perhaps by an additional Order to account for CUI. This would be a multi-disciplinary task, perhaps chaired by the Information Security Oversight Officer, that would start with the philosophy of need that exists today, rather than that which has carried forward from World War II.

This task will be difficult for many reasons, not the least of which is that more than the three branches of the federal government should be involved. It should include state and local representatives, private industry and academics. It will also be difficult because it is a truism that too many cooks spoil the broth. Finally, it will be difficult because those who must create this scheme may not truly represent the bulk of the American people. Those who have significant access to information obtain that access, in part, by sacrificing a great deal of the privacy to which the ordinary citizen is entitle. We need to keep in mind that those who do not enjoy the full guarantees of privacy many not understand fully how important those guarantees may be to others. We will have to take care that, in creating a scheme that will make information available, we do not create an access regime that would strip away the privacy guarantees most important to individuals.

Despite the obvious difficulties, the need is real and of such a magnitude that changes to our heritage of information restrictions simply cannot be placed in the "too hard" box. We must update our philosophies of access and control, change the guidelines that proceed from those philosophies and strictly control the use of unclassified caveats.

CONCLUSION:

What is recommended here is a series of tasks that may take several years before anything approaching a culminating effort can be effected, but each element can proceed along its own path at any time. Already, elements of this task are moving forward under both Presidential and Director of National Intelligence guidance stemming from the Intelligence Reform Act of 2005. A program manager (PM) for an Information Sharing Environment (ISE) is considering many of the issues. The Information Security Oversight Office is considering a re-write of the classification Order.

The results of these, and similar efforts, will be helpful, but they will not "turn the corner." If we are to succeed in the long run, a new approach, based on an updated philosophy of information restriction and disclosure is required. All of us who have worked under the current standards, many for decades, will understand how difficult this task is. The question is whether those with the ability to apply an updated information philosophy that can address the security of the nation will do so. We have entered an era radically different from the one in which those individuals (the author included) spent their formative years – with many urgent and pressing tasks already on their plate, it will take significant focus for them to realize how necessary, and how urgent the task is.

M. E. "Spike" Bowman, Esq., Capt., USN(Ret) is currently at the Center for Technology and National Security Policy at National Defense University. He recently retired from his post as Chief, Intelligence Issue Group, Federal Bureau of Investigation. Previously, as Senior Counsel, National Security Affairs, he was responsible for legal issues arising from traditional and economic espionage, for international and domestic terrorism, and for international organized crime and threats to the information and other critical infrastructure of the United States. Currently he is responsible for policy issues arising from intelligence process and operations and for information sharing. He is a long-standing life member of AFIO and serves on the AFIO Board of Directors.

After two years in Washington, I often long for the realism and sincerity of Hollywood.

— Senator Fred Thompson, who also acts in numerous TV shows and Movies, in Speech before the Commonwealth Club of California