Center for Public Policy and Private Enterprise
School of Public Policy, University of Maryland

The Unintended Audience: Balancing Openness and Secrecy

Crafting an Information Policy for the 21st Century

BY
JACQUES S. GANSLER AND
WILLIAM LUCYSHYN

The Unintended Audience: Balancing Openness and Secrecy

Crafting an Information Policy for the 21st Century

by

Jacques S. Gansler and William Lucyshyn

September 2004

This research was conducted with the support of
The Center for Technology and National Security Policy
National Defense University

****

The views expressed in this report are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

****

Comments pertaining to this report are invited and should be forwarded to:

Director
Center for Public Policy and Private Enterprise
2101 Van Munching Hall
College Park, MD, 20742

Comments may also be conveyed directly to either:

Dr. Jacques S. Gansler
301 405-3563
jgansler@umd.edu

or

Mr. William Lucyshyn
301 405-8257
Lucyshyn@umd.edu

Abstract

Certain public, private, and academic/scientific information exists outside the scope of security classification even though it poses threats to national security and public safety—for example, medical research on vaccines can unexpectedly yield new, deadly pathogens. It is in this ill-defined area that some forms of controls are most needed, yet most controversial. This paper first reviews the many and varied legislative and executive department and agency policies that have evolved to control this information. With the goal of defining a comprehensive policy to govern truly sensitive information—yet with a preference for maximizing openness—the authors argue for a system of Controlled Unclassified Security Information (CUSI), where a mixture of regulation, cooperation, and review, balanced with sector-specific values, optimally unite to manage highly-selective and well-defined sensitive areas. Beyond these specific, sector-level mechanisms, three overarching elements—namely, educational campaigns, an appeals process, and international control of sensitive information—help bring the CUSI system to a cohesive whole. The paper concludes by proposing metrics for assessing the overall effectiveness of the policy.

The Unintended Audience: Balancing Openness and Secrecy

Executive Summary

As the nation continues to combat global terrorism, the government is forced to reevaluate the balance between openness and secrecy when controlling unclassified, but sensitive, information. Certain information originating in the public, private, and academic/scientific spheres exists outside the scope of security classification even though it poses threats to the national security more broadly conceived. It is in this ill-defined area that some forms of controls are most needed, yet most controversial. The government's still-unstated policy objective can be understood as moving from this broad desire to comprehensively limit access to sensitive, unclassified information, to the more focused goal of ensuring security by restricting access to unclassified information that could be used by an adversary, adversarial group, or nation to develop or employ weapons of mass destruction or pose a manifest threat to public safety.

Yet this whole process must be undertaken with extreme caution. The great value of openness of knowledge is a recognized, accepted, and critical part of a free and democratic society—and it is clearly of great societal and economic benefit. Therefore, the restrictions applied must be extremely limited and—even in the case of doubt—must be biased in favor of openness.

The difficulties of defining and implementing a comprehensive policy to govern truly sensitive information are reflected in the many and varied information security policies that have evolved. Having numerous competing policies from Congress and executive department and agency sources makes the task of discerning what is—and how to handle—"sensitive information" particularly difficult, especially because the policies themselves often are confused. It is not surprising that there has been a mixed tradition of expanding and relaxing controls on unclassified, sensitive information in reaction to changing perceptions of threats.

The first step in consolidating, coordinating, and refining existing policies aimed at protecting unclassified, sensitive information is to develop a clear understanding of what information should be identified and controlled. The president, in consultation with the Department of Homeland Security (DHS) and the Department of Justice, should issue an executive order that identifies the types of information—namely, information relating to weapons of mass destruction, critical infrastructure information, and intelligence and security information—that could be designated Controlled Unclassified Security Information (CUSI). The values that constrain regulation are particular to each sector. Linking the policy's definition to the sector-specific values—such as openness, autonomy, and academic freedom—allows for finely-tuned, appropriate implementations. While the definitions of what categories of information potentially are sensitive remains constant and implies a need for controls, the same controls are not appropriate in all sectors, nor is all the information in any category automatically sensitive. Of course, determining where the information originates and resides affects the control options available to the government.

For sector-specific guidelines, we make the following recommendations:

- *Public sector regulation* should focus on coordinating, consolidating, and sharing information generated and controlled by the government. As such, government departments and agencies should consistently implement a single, presidentially-defined government-wide policy for Controlled Unclassified Security Information (CUSI), and it should enable the sharing of sensitive materials between departments and agencies at the federal, state, and local levels, as well as with those in the private sector with a need-to-know.

- The government's *cooperation with the private sector* should be geared toward creating incentives for private companies to share information so that the government can analyze interdependencies and potentially mitigate vulnerabilities. The Department of Homeland Security's Directorate of Information Analysis and Infrastructure Protection should lead the effort to define and collect sensitive private-sector information.

- The *review of the academic/scientific sector* should encourage constrained research and publication for both federally-funded and non-federally-funded work in highly sensitive areas. DHS, in conjunction with other federal departments and with support from the National Science Foundation (NSF), should create and run education and awareness campaigns for both researchers and publishers that foster a spirit of institutional and professional responsibility to curb research into and publication of imminently dangerous information. Federally-funded researchers should disclose potential security concerns in their grant proposals. DHS-monitored review panels will assess the security implications of the work with potentially significant negative impact in accordance with established guidelines. DHS should lead the effort to develop model review policies, encouraging non-federally-funded researchers to adopt them and to submit their work to the government-monitored review panel or an independent, government-certified review panel. DHS should also train publishers to conduct reviews just before research is made available to serve as a safety net after research is already completed, and publishers should implement a two-tiered publication scheme to restrict detailed content to premium access where the credentials of the readers can be verified.

Beyond these three specific sector-level mechanisms, three overarching elements help bring the CUSI system to a cohesive whole:

- First, the Under Secretary of Information Analysis and Infrastructure Protection in the Department of Homeland Security should lead the effort to *educate key personnel*—including journal editors, review staff, security officers, researchers, etc.—with the concepts, rules, and guidelines of CUSI. Specifically, the workshops should have three objectives: to publicize sector-specific guidelines, to raise general awareness of security concerns, and to educate people so that they can measure the "work-factor"—that is, a metric for measuring the costs of obtaining and the convenience of using specific information—for leveraging potentially harmful information.

- Second, DHS and the National Archives and Records Administration (NARA) should *administer an appeals process* that has a clear vision and a mandate for openness, allowing for individual decisions about the categorization of information to be reviewed on a case-by-case basis.

- Third, the *international component* must address creating similar policies abroad as well as continuing to attract foreign students and researchers. Proposals for the international regulation of sensitive information should be taken abroad via all available channels after the domestic system operates with the confidence of policymakers, scientists, and the public. The State Department and the U.S. Citizenship and Immigration Services (USCIS) should publicize and build on the successes most foreign students are having in the United States to continue to attract talented students while communicating the details of new programs and procedures to prospective and current students. Impacts from policy changes must be closely monitored and policies adjusted as feedback becomes observable.

As the CUSI policy is put into place, it will be important—but somewhat difficult—to analyze the success of the policy because of the many dimensions involved, and to continuously improve the details of the policy through the lessons learned. To do this, we recommend a system of analysis that assesses the policy's performance in each of five categories, taking into account the differences between the public, private, and academic/scientific sectors. The first two metrics focus on miscues in the CUSI designation process relating to false identifications and false disclosures, whereas the latter three focus on somewhat less tangible aspects of the CUSI policy, including the extent of government involvement, research and development potential, and overall feasibility of the policy. Together, these metrics should imply the effects that perceived threats are having on the real benefits of research. The Directorate of Information Analysis and Infrastructure Protection of DHS should continuously evaluate the extent to which designating material CUSI increases security but leaves information accessible to those who need it, and it should continuously evaluate the review and appeals processes to ensure that standards are moving neither toward excessive secrecy nor imprudent openness.

Policy makers have faced considerable challenges in trying to craft a coherent information security policy because of the lack of a comprehensive strategy for governing sensitive information in the public, private, and academic/scientific sectors. However, the problem can be decomposed into manageable parts. As a first step, it is necessary to identify sensitive areas that potentially affect security. Then, controls can be developed and implemented at the sector level, accounting for the values that limit the controls that can be placed on each sector. Together with educational campaigns and a working appeals process, these parts can be used to influence an international audience to encourage thoughtful information security that makes the global society safer without diluting its valuable intellectual base.

Section I: Introduction

To every man is given the key to the gates of heaven;
the same key opens the gates of hell.

—Buddhist proverb quoted by Richard P. Feynman

As the nation continues to combat global terrorism, the government is forced to reevaluate the balance between openness and secrecy when controlling unclassified, but sensitive, information. Certain information originating in the public, private, and academic/scientific spheres exists outside the scope of security classification even though it poses threats to the national security more broadly conceived. Material posted on government Web pages might provide terrorists with information they could use to plan attacks. The location and vulnerability of nuclear facilities or a chemical plant with highly toxic material and a very poor safety record might be good terrorist targets. A scientific journal publishing papers on how to make human, animal, or plant diseases more virulent may enable terrorists to create biological weapons capable of attacking specific populations and food supplies.

There has been a mixed tradition of expanding and relaxing controls on this type of unclassified, "sensitive" information in reaction to changing perceptions of threats. It is in this ill-defined area that some forms of controls are most needed, yet most controversial. At the center of this issue rests the problem of first defining what information truly is sensitive and then identifying ways to control it. Paradoxically, any definition must be sufficiently broad to capture the full range of vulnerabilities while remaining sufficiently narrow to avoid both potential abuses and/or unnecessary restrictions that slow the development of the nation's intellectual capital.

The difficulties of defining and implementing a comprehensive policy to govern truly sensitive information are reflected in the many and varied information security policies that have evolved. The current administration has not made explicit its motivation behind controlling sensitive homeland security information.[1] However, we can infer that there is a desire to place restrictions on unclas-

[1] Former Bush Administration Chief of Staff Andrew Card made it clear that "government information, regardless of its age, that could reasonably be expected to assist in the

sified information that could be used by a potential adversary, adversarial group, or nation to develop or employ a weapon of mass destruction (WMD), or pose a manifest threat to public safety.

This paper attempts to identify what sensitive information ought to be controlled, describe who ought to control it, and enumerate the mechanisms through which it should be controlled, while balancing the levers through which the policy is implemented with the values that underlie each sector. These policies are driven by a dynamic between government regulation, industry cooperation, and peer review that are checked by an appeals process. When taken as a whole, these policy mechanisms lay the groundwork for future cooperative international regulation. Ultimately, we offer a definition for controlled unclassified security information in order to coordinate information flows in and among the public, private, and academic/scientific sectors.

The Tradition of and Need for Openness

The United States enjoys a long tradition of openness and transparency in government that has its heritage in the Constitution. The separate institutions sharing powers (Neustadt 1991) create a constant struggle and need for information between the branches of government. Moreover, the rights guaranteed by the First Amendment enable the press to serve as a proxy for the public by representing their concerns and serving as a watchdog. Even as the scope of government grew throughout the late 1800s and early 1900s, Congress refused to allow the executive branch to impose official secrecy on the increasing number of federal agencies. Consequently, only information that would pose a direct threat to national security if released could be restricted with security classification.

The tension between the executive and legislative branches persisted, the scope of government expanded still further, and the amount of information the government kept secret under the auspices of protecting the national security increased. However, as a check on the growing amount of information withheld, Congress passed the Freedom of Information Act (FOIA) of 1966, which enables individuals to request the disclosure of information not ordinarily available to the public. According to the FOIA provisions, in order for the government to restrict information, it must meet one of nine allowable exemptions specified by the law—for example, containing a pre-decisional or deliberative attitude of the government, or potentially compromising an ongoing law-enforcement investigation

development or use of weapons of mass destruction . . . should not be disclosed inappropriately." The federal government, who "collects, creates, manages, and protects" sensitive homeland security information, has a responsibility to safeguard and share it with state and local personnel "to prevent and prepare for terrorist attack," as stipulated by the Homeland Security Act.

or operation (Department of Justice 2002a). These provisions were augmented in 1976 with the passage of the Sunshine Act, which required federal agencies to open more of their meetings to the public. FOIA itself was amended several times, most significantly in the amendments of 1974, further reforms in 1986, and updated in 1996 in order to narrow the scope of law enforcement and national security exemptions, to enact substantive and procedural reforms, and to address "electronic record" issues, respectively.

Apart from its legislative history, the case for openness has been articulated and strengthened by a number of executive orders and actions. President Ford's Executive Order 11905 restricted intelligence activities and established an Intelligence Oversight Board. President Carter's Executive Order 12605 changed the definition of the security classification "confidential" to include "identifiable damage" rather than simply "damage," and it identified seven areas in which information could be classified. Most importantly, it established a balance test to determine if public interest outweighed possible damage to national security. The Carter Executive Order also continued automatic declassification and established the Information Security Oversight Office (ISOO) to monitor agencies' compliance.

President Reagan issued National Security Decision Directive (NSDD) 189 in 1985, affirming the basic openness of fundamental scientific research. More recently, Condoleeza Rice, the National Security Advisor, reaffirmed NSDD-189, stating that the "linkage between the free exchange of ideas and scientific innovation, prosperity, and U.S. national security is undeniable" (Rice 2001).

Underlying Normative Considerations: Knowledge and Information Technology

Lingering behind current information policy issues is the more abstract, long-standing question about the desirable limits to the discovery of knowledge itself. The advancement of science in fields that have tremendous potential to do both good and harm raises questions about the ends of scientific discovery. Reinforcing the potential danger of certain knowledge is the emergence of the information age where the transmission of such powerful information is easier, faster, virtually no-cost, and in many ways less secure than ever before.

Determining whether and how best to limit access to information raises issues relating to the purposes of knowledge. Contemporary thinking suggests that knowledge itself is benign but that its applications are not. Moreover, it is not clear whether knowledge is an end in itself that should be pursued or if it is a means to some other end, such as improved social welfare. In the former case, if knowledge has intrinsic worth, then restraining the discovery of new knowledge or constraining the transmission of knowledge in any way is ultimately harmful to society. However, if acquiring knowledge is simply a means to an end, as in the latter case, then there are strong theoretical reasons why knowledge should be constrained or even restrained. Inspired by his observations when flying a B-25 airplane over Hiroshima shortly after the atomic bomb was dropped, Roger Shattuck makes the case that limits and restraints on knowledge can have value for society by citing a long literary tradition beginning with the Greek mythological story of Prometheus (Shattuck 1997).[2] The moral of this myth—in which man is given both fire for his assistance and a box containing all of the world's troubles—is that an advancement of any kind can have both positive and negative results.

Constraining knowledge may not only be beneficial, but even imperative. In *The Presumptions of Science*, Robert L. Sinsheimer makes an even stronger case for the need to restrict knowledge. He argues that some values are more important than the intrinsic goodness of knowledge. This conclusion suggests that society should attempt to regulate knowledge to an optimal level, relative to its social context (Sinsheimer 1980).

A contemporary complication to concerns about the potential dangers of knowledge is the emergence of the computer, the Internet, and the information revolution. Unlike the relatively slow dissemination of information restricted to the printed page, today information can be available in real-time to virtually anyone on the planet. However, the introduction of technology translates into differences in degree rather than substance—that is, knowledge is still knowledge, though it is spread faster. As such, the moral dilemma of whether and how to regulate knowledge is still the same. To be explicit, technology can be either a tool that enables the spread of a good with intrinsic value, or an unstoppable force that abets a process that otherwise should be restrained—it does not change the nature of the information.

In reality, determining the nature of knowledge is not a simple binary choice between ends and means. Instead, we accept that knowledge is both an end in itself as well as a means to other ends. Simply put, there is some knowledge that plainly is worth having, while other knowledge is useful for other more immediate purposes—both negative and positive. Therefore, in crafting an information policy for the 21st century, we must be careful to constrain rather than restrain—that is, the salient policies must allow the avenues of discovery to be policed

[2] Prometheus, the greatest of the Greek Titans, whose name means "foresight," created man. He stole fire from Zeus and his son Hephaestus, the blacksmith, to give to mankind so it could sustain its civilization. In Hesiod's version of the myth, Zeus punished mankind by sending the first woman, Pandora, whose name means "giver of all." Pandora opens a box that contains all the world's troubles, negating the benefits of fire. In the Aeschylean version, Prometheus is bound to a mountain where an eagle eats his liver everyday.

without erecting permanent roadblocks.[3] However, in the absence of a clear warrant for its control and based on our democratic traditions, the default policy must allow knowledge to move freely and openly.

Practical Reasons for Scientific Openness and Collaboration: The Soviet Experience

The case of research and development within the Soviet Union during the Cold War is an example of the pitfalls of an overly-restrictive, security-related information sharing process. The Soviet system intentionally limited the transfer of information both within its own scientific communities and with communities abroad. Arthur Alexander's extensive study demonstrates that Soviet policies tended to break down the links between research, design, and development necessary for successful innovation (Alexander 1988). Additionally, analysis of the 1986 Chernobyl nuclear power plant accident suggests that secrecy can be dangerous in a technical society, because openness is necessary for both preventing and responding to accidents (Shlykhter 1992).

Science was, in effect, subordinated to the state through the imposition of excessive secrecy. Collaboration, an essential part of effective research, was suppressed both domestically and internationally. Soviet academicians and scientists envied the "invisible colleges" of the West, and they often had to rely on the West to verify their research results because research was extensively compartmentalized (Alexander 1988). Moreover, the institutional barriers between organizations and sectors not only disrupted the transfer of knowledge, but also limited the serendipitous synergy of ideas that produces the most meaningful advances. The Soviet penchant for secrecy thus artificially restrained the advancement of science, guarded the thinking of academicians and scientists, and limited the ability to prevent and respond to accidents.

Restricting information and investigation limits discovery. Discoveries, of course, may be helpful, harmful, or both. Indeed, as terrorists become more creative, an increasing amount of information has this fundamental dual-use nature—for example, pharmaceutical research is both helpful because it provides treatment and harmful because it may detail how infectious diseases are spread. There must be a level of openness so that researchers can fully engage science—by collaborating, building upon each others' research, and verifying experimental outcomes—while maintaining fundamental security. Security measures, where necessary, should be *con*straints rather than *re*straints—that is, limits rather than prohibitions—to ensure that the necessary and jointly sufficient means of knowl-

[3] Throughout this paper, we use "constrain" and "restrain" to connote the processes of "limiting" and "actively prohibiting," respectively.

edge, skill, and resources—as enabled by the values of openness and collaboration—ensure the ends of healthy scientific advancement.

The remainder of this paper discusses the need for a more cohesive information policy, reviews the extant legislative and regulatory controls for sensitive information, discusses current efforts to limit sensitive information, and recommends and assesses a policy for controlling sensitive homeland security information.

The Need for a Unified Sensitive, Unclassified Information Policy

Executive Order 12958 provides specific guidance for determining what information can be classified to protect national security.[4] However, there is also much information that either does not meet the criteria in this EO, does not meet the threshold specified, or, for pragmatic reasons, cannot be classified but should still be restricted. Thus separate sets of regulations have evolved to control this type of unclassified, sensitive information outside of the classified national security information scheme. These separate sets of controls are necessary, as the information warrants a degree of protection, albeit at a level less than and different from classified. For example, personnel rosters or medical data do not warrant the same level of protection as nuclear weapon design data.

Existing Legislative Controls on “Sensitive” Information

Much of the relevant legislation—especially relating to today’s concerns about weapons of mass destruction—focuses on the post-World War II effort to secure information pertaining to the development of nuclear weapons. The Atomic Energy Act of 1946, which was later revised in 1954, established that “restricted data”[5] is subject to secrecy from the moment of its creation, even though its creator might be a private individual—that is, restricted data is “born classified,” regardless of who produces it and how it is produced.

The Export Administration Act of 1979 and Arms Export Control Act of 1976 were intended to regulate the exportation of dual-use items—items that have both civil and military applications—in addition to sales of goods with direct military applications, by requiring export licenses. These laws also authorized the control of “scientific data” related to these items. Under these acts, the

[4] EO 12958, entitled Classified National Security Information, “prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.”

[5] Restricted Data is complex, critically sensitive, technical information concerning nuclear weapons design and utilization and the production of fissile material, such as weapons-grade isotopes of uranium or plutonium.

Department of Commerce was given the responsibility for establishing and controlling the Export Administration Regulations (EAR), while the State Department controls the International Traffic in Arms Regulations (ITAR). The Department of Defense advises both the Commerce and State Departments. Agencies operating under these laws can impose controls on *government-sponsored* unclassified university research in the form of pre-publication review and restraints, including sanitization of data, publication restraint, classification, etc. For example, DOD forced the withdrawal of one hundred documents at a meeting held by the Society of Photo-Optical Engineers in 1982 (Relyea 2003). International partners may be barred from participating in certain sensitive research activities because U.S. officials perceive a domestic advantage that they are unwilling to share. This may be harmful both because the United States may be excluding the best researchers and because the assessment of the state of U.S. vis-à-vis foreign technology in certain fields may be incorrect—other countries may have a technical advantage.

The Invention Secrecy Act of 1951 enables Departments of Energy (DOE), Justice (DOJ), or Defense (DOD) agency heads to request a one-year patent secrecy order if they think that disclosure might harm the national security. Secrecy orders may be extended in one-year increments if the agency head determines that it is in the national interest to do so, and there are also provisions for extending secrecy orders in times of war. Extensions are common—of the 4,838 secrecy orders in effect at the end of fiscal year (FY) 2003, only 133 were issued during that year. Only eighty-seven secrecy orders were rescinded during FY 2003 (Invention Secrecy Activity, U.S. Patent and Trademark Office, FY 1999–2003 2004). Additionally, inventors must obtain a license before filing a foreign patent for a U.S.-made invention.

The Secretary of Defense can withhold technical data associated with military or space applications under the Defense Authorization Act of 1984. However, the data must be under the control of DOD, and it must be subject to export controls. Additionally, patent secrecy orders may cause problems related to international information asymmetries. For example, inventors may claim that their patents are being infringed upon by foreign competitors, but the U.S. Patent and Trademark Office (USPTO) may not release the information necessary to litigate because of perceived negative security implications. The disconnect between the USPTO and agency officials and the works in question may lead to decisions to err on the side of security, often to the detriment of the inventor.[6]

One of the more recent attempts to control sensitive information through legislative action was the Computer Security Act of 1987, which formed a govern-

[6] Under the Invention Secrecy Act, inventors are entitled to "compensation for the damage caused by the order of secrecy and/or for the use of the invention by the Government [sic]."

ment-wide program to establish security for computer and communication systems. Under this system, the National Bureau of Standards (NBS) [7] was given responsibility for establishing standards and guidelines for information security and privacy, and it was charged with training employees. Most importantly, the Computer Security Act contains a government-wide definition of "sensitive but unclassified" (SBU) information. The definition—"information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests"—is identical to both the controversial 1984 White House issued NTISSP 2 memo[8] (Knezo 2002) and DOE policy (Office of Security Affairs and Office of Safeguards and Security 1995).[9] Although Congress had the Reagan Administration rescind the definition in NTISSP 2 because of concerns regarding the broad scope of the information that could be controlled outside of national security interests and the responsibility given to the intelligence community over civilian information activities, the wording is still present in the Computer Security Act and has remained DOE policy.

Other Controls on "Sensitive" Information

Executive departments and agencies often place controls on the sensitive information that they manage, but frequently these designations and controls do not easily overlap or correspond to the measures being taken in other departments and agencies. Individual departments and agencies have been defining sensitive information according to their information security needs. Having numerous competing policies makes the task of discerning what is—and how to handle—"sensitive information" particularly difficult, especially because the policies themselves often are confused (Department of Defense 1997).[10] For example,

[7] The National Bureau of Standards was renamed the National Institute of Standards and Technology (NIST) in 1988 as part of the Omnibus Trade and Competitiveness Act.

[8] In September 1984, National Security Advisor John Poindexter sought to expand the definition of sensitive but unclassified in the National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems (NTISSP No. 2). This expansion would include information that could adversely affect "other government interests," in addition to national security.

[9] The definition of "sensitive unclassified information" as given in the Safeguards and Security Glossary of Terms is identical to the Computer Security Act's definition.

[10] For example, Appendix 3 of the Information Security Program DOD 5200.1-R notes that additional information known as "unclassified controlled information" exists alongside of classified information. The DOD regulation indicates that SBU information—and therefore information that was previously labeled LOU—shall be marked, handled, and secured according to the same procedures as FOUO information. SBU information does not require the carrier to be informed of the controls. Interestingly, this explicitly applies to SBU information that originates within the Department of State—no mention is made of controlling information designated SBU that originates elsewhere.

some agencies use the “sensitive but unclassified (SBU)” label interchangeably with “For Official Use Only (FOUO),” or “Limited Office Use (LOU).” In fact, there are at least fifty-two different protective markings being used by departments and agencies on unclassified information, and approximately forty of these markings are used by agencies and departments that also classify documents (Senate 1997).

The lack of coherence between policy-making bodies is evident in the Federal Energy Regulatory Commission solicitation for public comment regarding its Critical Energy Infrastructure Information (CEII) policies (Federal Energy Regulatory Commission 2004). These policies, enacted shortly after September 11, attempted to establish a system for protecting information that was once publicly available as well as detailed information regarding both currently “licensed and certificated” and proposed facilities. The Commission’s policy does not completely mesh with existing policy, nor does the announcement acknowledge the Department of Homeland Security’s broader, government-wide attempt to control all critical infrastructure information. DHS attempted to describe the relationship between Protected Critical Infrastructure Information (PCII) and “other similar regulations,” including CEII, in its Procedures for Handling Critical Infrastructure Information Interim Rule (Department of Homeland Security 2004). However, the document notes only that the cases in which both sets of rules will apply are expected to be few, and it proceeds to contrast the mechanisms through which the different types of information are protected, shared, and released.

Similar to the EAR and ITAR regulations, the Treasury Department’s Office of Foreign Assets and Control (OFAC) is charged with enforcing U.S. sanctions on embargoed countries. Although the Berman Amendment of 1994 allows the *export* of “information and informational material,” publishers in the United States cannot edit articles submitted by citizens of embargoed countries. For example, the Institute of Electrical and Electronics Engineers (IEEE) finds it almost impossible for foreign-produced works to appear in their publications without special licenses (Kumagai 2003).[11] IEEE membership in embargoed countries has fallen from seventeen hundred to two hundred, and members cannot enjoy some of the organization’s benefits, such as accessing online job listings and conducting conferences under the IEEE name. The penalties for failing to comply with OFAC guidelines are up to $10 million and prison terms. The OFAC policy seems counterintuitive, as security experts should be consulted with regard to information both *going to* and *coming from* certain countries. However, OFAC’s policies allow much of the domestic cutting-edge research to be released without intervention, potentially aiding adversaries, while also preventing domestic security experts from monitoring scientific advances abroad, restricting the flow of

[11] *IEEE Transactions on Electron Devices* has carried only two articles by Iranian researchers this year.

scientific information, and discouraging collaboration.

The Changing Nature of Threats

Modern and Contemporary Threats: From Centralized to Distributed Attacks

The modern, post-World War II history of controlling information to mitigate threats to the national security focused on restricting the flow of information to the Soviet Union. The public generally was unwilling to accept the government's periodic attempts to impose controls on more nebulously defined unclassified, sensitive information, particularly during the 1980s and especially regarding scientific information. After all, throughout the Cold War, the enemy was easily identifiable and restrictions were in place and visible. Restricting the flow of information with national security implications was limited to processes undertaken by the two superpowers and their allies. Bilateral efforts primarily were focused on maintaining the equity of nuclear and conventional arsenals, while secondary efforts were made to control proliferation and slow the development of weapons and weapons systems among a host of easily identifiable states.

The current threat of transnational terrorism is much different, and it has reopened the debate on the control of sensitive information. The contemporary problem of ensuring homeland security is particularly acute because the threats are now seen as highly distributed rather than emanating from one source. Additionally, terrorist networks are able to extend to new markets because information technology advances and global economic integration establish additional points of entry, creating new targets for and avenues of attack. As the events of September 11 and the subsequent anthrax attacks demonstrated, terrorists can be exceptionally creative and effective when their objective is inflicting mass casualties. With many different adversaries attempting to gain access to weapons of mass destruction to exploit these myriad points of vulnerability, many lawmakers believe that there are now good reasons for restricting access to potentially harmful unclassified, sensitive information.

At the same time, science is developing new capabilities so rapidly that our ability to fully understand their impacts and evaluate their consequences may not be able to keep pace.

The Focus on Biological Weapons

Significant breakthroughs in the life sciences, especially those relating to the structure and function of genes, have significantly increased the ability to develop biological weapons. Although terrorist groups are also trying to acquire nuclear and chemical weapons, concern within the government and among the public has focused primarily on biological weapons (Bolton 2002). The barriers to a small group developing and successfully delivering a nuclear weapon are high because of the enormous resources required to enrich uranium, design and produce a functioning warhead, and acquire delivery mechanisms.[12] And, even though chemical weapons may be easier to manufacture than nuclear weapons, their use is very localized and disperses relatively quickly. Additionally, when creating terror, being "gassed" by a chemical weapon does not convey the same horror as being "infected" by a biological weapon (Terror in Tokyo 1995; Bilski 1995; Harmon 2003).[13]

In some ways, it is easier to demarcate which aspects of biotechnology could be used against the United States compared to other potentially dangerous technologies. Indeed, the National Academies of Science have identified seven key areas of biotechnology research that are most harmful (Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology 2003).[14] However, bioweapons are hard to detect, partly because of the dual-use nature of the facilities needed to conduct research and produce them, and partly because of the low intellectual and material startup costs. Low startup costs, in turn, lead to a real and perceived short lag-time between research in the biological sciences and its applications, thus making them more attractive to terrorists and increasing their perceived threat.

Although many people are worried about the spread of genetically-altered germs, George Poste claims that "bugs are only the tip of the bio-iceberg." A growing fraction of the whole field of biotechnology—for example, recombinant DNA technology—can be used to develop more virulent agents that exploit specific biochemical features and induce specific effects (Poste 2003).[15] According to the same National Academies study, many of the skills needed for using recombinant DNA techniques are taught routinely in high school biology courses,

[12] If these groups can gain access to enriched fissile material, these costs are reduced, but they still are not trivial.

[13] Sarin gas, which was used in the 1995 terrorist attacks in a Tokyo subway station that killed ten people and injured over five thousan d, can be produced from components available from any chemical supply company relatively cheaply. A fatal dose is about .01 milligrams per kilogram of human weight, and it kills within minutes by paralyzing the respiratory system.

[14] The seven categories concern experiments that would demonstrate how to render a vaccine ineffective; would confer resistance to therapeutically useful antibiotics or antiviral agents; would enhance the virulence of a pathogen or render a nonpathogen virulent; would increase transmissibility of a pathogen; would alter the host range of a pathogen; would enable the evasion of diagnostic/detection modalities; and/or would enable the weaponization of a biological agent or toxin.

[15] For example, an agent that stimulates an excess in the natural production of insulin could cause an overproduction and lead to hypoglycemia, causing blurred vision, headache, fatigue, dizziness, irritability, increased heart rate, shaking and tremors, and hunger (Diabetes Education and Research Center 1999). At a low level, such an agent would be a nuisance, keeping people from concentrating. At an acute level, it could lead to loss of consciousness, seizure, coma, and death.

and they are certainly within the skill set of most biology graduate students.

Because the equipment and processes needed to produce advanced biological weapons are dual-use, it is difficult to differentiate a legitimate research activity from weapons development. Also, biological weapons research and production is much easier to hide than an analogous nuclear program. Even considering the small, well-hidden, largely indigenous South African nuclear weapons program, only one or two nuclear weapons could be produced a year (Albright 1994) with annual operating costs of $6 million to $7 million (Schwartz 1998). South Africa's civilian nuclear program, on which the weapons program was based, required significant assistance from abroad (Schwartz 1998). On the other hand, David Kay, in his interim progress report on the activities of the Iraq Survey Group, indicated that scientists stored vials of biological agents in their homes; pharmaceutical facilities could have been converted to produce anthrax within one week if the seed stock were available; and laboratory equipment was concealed in a mosque (Kay 2003).

Also, bio-systems are unpredictable because they self-propagate and evolve. It might be difficult to close a Pandora's Box opened through accidental discovery, unintentional alteration, or terrorist activity (Allewell 2003). For example, an experiment that inadvertently increased the virulence of mousepox keenly raised awareness of the dangers of biological research (Jackson 2001; Weiss 2003). Mark Buller's federally-funded research increased the virulence of mousepox, though his work did so intentionally to find a treatment that would work against it. In response to concerns that his research posed a threat to humans, Buller claimed that he has "absolutely no biosafety issues" because his work does not infect humans, although someone theoretically could employ the same technology to create a more virulent form of smallpox. In another experiment, Eckard Wimmer and others synthesized poliovirus from information found on the Internet and mail-order materials, again causing concern among policy-makers (Cello 2002). While this process took three years, an Institute for Biological Energy Alternatives project, sponsored by DOE, synthesized a comparably-sized, self-replicating virus in two weeks—and the methods and results have been published in the *Proceedings of the National Academy of Sciences* (Weise 2003).[16] Stories like these lead lawmakers and the public to believe that biological weapons are easy to develop and deliver. Underscoring this point, Buller is quoted with saying, "The things we did to make that virus more virulent is kindergarten stuff." Anthony F. Fauci, director of the National Institute of Allergy and Infectious Diseases, the part of the NIH that funded Buller's work, goes a step further in pointing out, "Everybody knows how to do this. The hard part is figuring out

[16] The article was made available online on December 2, 2003 and in print in the December 23, 2003 issue of *Proceedings of the National Academy of Science*, under the title, "Generating a synthetic genome by whole genome assembly: ΦX174 bacteriophage from synthetic oligonucleotides."

how to counter it."

A single terrorist intending to poison a water supply could produce and conceal numerous vials of dangerous agents in his living room. Again, this can be contrasted with the South African nuclear experience, where the manufacture of "deliverable gun-type devices" required a disguised, two-story structure with a total of eight thousand square meters of floor space (Albright 1994). The facility required one hundred employees in the early 1980s and the workforce rose to three hundred by 1989. Consequently, the perception exists among policymakers that many people are willing to accept greater controls on sensitive information coming from scientific research, especially in the field of biotechnology.

Reactions to the Attacks of September 11

The Bush administration has taken several steps subsequent to the events of September 11 that have impacted the availability of information (Ashcroft 2001). These include issuing a memorandum specifying this administration's interpretation of the Freedom of Information Act (FOIA); restricting "sensitive but unclassified" information, especially as related to weapons of mass destruction; requesting that government agencies remove "sensitive information" from their websites; taking steps to secure scientific research and academic institutions by encouraging self-censorship; and limiting the number of foreign students attending American academic and research institutions.

Reinterpreting the Freedom of Information Act

An October 12, 2001 memorandum from Attorney General John Ashcroft to the heads of Departments and Agencies was the first important change in information policy. The memorandum states that the Justice Department will support decisions to withhold information from FOIA requests as long as it is legally justifiable (Ashcroft 2001). This is a fundamental change in policy from Janet Reno's 1993 memorandum, which advised openness unless a clear reason for retention could be given. The Reno memorandum established that non-disclosure should take place only when it was "reasonably foreseeable that disclosure would be harmful" (Reno 1993). The Ashcroft memorandum assures agency and department heads that "the Department of Justice will defend [their] decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records" (Ashcroft 2001). The policy shift represents a clear decision, when sensitivity is questionable, to err on the side of security rather than on the side of openness. However, the verbiage in the Ashcroft memorandum—to withhold as long as there is "sound legal basis" to do so—still maintains an important feature of the Reno memorandum—that of discretionary disclosure.

Ashcroft's memorandum was in draft form long before the events of September 11, it did not change significantly afterwards (Metcalfe 2003), and it followed in the spirit of previous memos. Specifically, in 1976 Attorney General Bell established the basis for nondisclosure when there was "demonstrable harm" (Department of Justice 1981b), Attorney General Smith in 1981 when there was a "substantial legal basis" (Department of Justice 1981a), and Reno in 1993 when there was "foreseeable harm." Moreover, on the whole, a National Security Archives study found that the effects of the Ashcroft FOIA interpretation have not been nearly as drastic as they were expected to be (Blanton 2003). The change in policy emphasis and tone therefore may fit in the context of both the administrative setting in which it was born and the post-September 11 world in which it exists.

Restricting Information on Weapons of Mass Destruction

Upon the request of former Bush Administration Chief of Staff Andrew H. Card, the Information Security Oversight Office (ISOO)[17] issued a memorandum on "Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security" to all government departments and agencies on March 19, 2002 (Kimberly 2002). In his cover memorandum to the Heads of Executive Departments and Agencies, Card made it clear that the government is seeking to clamp down on information relating to weapons of mass destruction (Card Jr. 2002). Card states that "government information, regardless of its age, that could reasonably be expected to assist in the development or use of weapons of mass destruction, including information about current locations of stockpiles of nuclear materials that could be exploited for use in such weapons, should not be disclosed inappropriately."

The two memoranda amend the guidelines for assessing government information and, most notably, urge all agencies and departments to "maintain and control sensitive information." However, neither memorandum explicitly defines what "sensitive information" means; rather, the ISOO memo describes it only as "information related to America's homeland security that might not meet one or more of the standards for classification set forth in Part 1 of Executive Order 12958." The responsibility for deciding what is sensitive is left to departments and agencies. Furthermore, the memoranda did not provide detailed guidance on *how* to maintain and control the information deemed "sensitive"—omitting, for example, possible special storage procedures and penalties for disclosure.

[17] ISOO is an administrative component of the U.S. National Archives and Records Administration (NARA). It is responsible for overseeing the government-wide security classification system and monitoring the national industrial security program. Specifically, ISOO disseminates security education materials, takes actions on appeals and complaints, recommends policy changes to the President, and provides program and administrative support for the Interagency Security Classification Appeals Panel. It receives its policy and program guidance from the National Security Council. ISOO's authority comes from Executive Orders 12,958 and 12,829.

In addition to these measures to control information regarding weapons of mass destruction, the USA Patriot Act of 2002 and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 expand control of those "select agents" that are deemed the most dangerous beyond human pathogens, to include plant and animal pathogens as well, bringing the total number of controlled pathogens to over seventy. Any laboratory that uses these agents must register and obtain permission to work with these agents. Employees who work with the select agents also must submit to background checks (Knezo 2003).

However, Senator Lieberman, who helped support the legislation, has noted a number of problems with its implementation (Mintz 2003). The Departments of Agriculture and Health and Human Services have not allocated sufficient funds to perform these checks—in fact, as of the beginning of November 2003, none of the laboratories or researchers has been deemed fully compliant, and only fifty-four hundred of nine thousand scientists have received limited security reviews. Additionally, of the estimated 1,653 labs and twenty thousand researchers who need certification, only 513 labs and nine thousand individuals have applied for approval. Although these figures have been disputed,[18] they still call into question the underlying implementation, measurement, and enforcement problems that the relevant departments and agencies must face.

Removing information from Government Websites

E-government—ways of delivering content and services to broad audiences through the use of information technology—took flight as the Internet became popular. Initial efforts by government at all levels were aimed at making information available to internal users (employees) and to citizens at large—the federal government maintains approximately one hundred million web pages at twenty-five thousand federal sites. DOD moved quickly to make virtually all unclassified data available online. "This included, what was in hindsight, sensitive data—like the floor plan of the Chairman of the Joint Chiefs of Staff's house in Washington DC; the operational status of Air Force Wings; and unit personnel rosters" (Gansler 2002). But much of the information that was put online was made available simply because it could be. As the nation's conception of terrorism changed in the late 1990s, government agencies, especially DOD, started pulling this kind of unnecessary information offline—well before the events of September 11, 2001.

This process accelerated significantly in the aftermath of the September 11 terrorist attacks. Different measures were taken by different agencies. The Nuclear Regulatory Commission temporarily shut down its entire site while it reviewed the posted content (Nuclear Regulatory Commission 2002). Information

[18] The accuracy of the figures has been disputed, though the claim that there are problems has not been challenged.

removed from the website during the review includes the exact geographic coordinates of nuclear plants (Ornstein 2001). The FAA removed certain databases, including its Enforcement Information System, which provides information on enforcement actions (OMB Watch 2002). The Office of Pipeline Safety discontinued open access to its National Pipeline Mapping System (Gugliotta 2001). The EPA removed Risk Management Plans (RMPs) that require industries to report potential chemical dangers (Gugliotta 2001).

In a related policy, federal depository libraries were instructed to destroy a CD-ROM entitled, "Source Area Characteristics of Large Public Surface-Water Supplies in the Conterminous United States: An Information Resource for Source-Water Assessment, 1999" (Gordon-Murnane 2002). The Department of Defense removed more than sixty-six hundred technical documents for review dealing with germ and chemical weapons, [19] and the Commerce Department removed about the same number of documents as part of an ongoing review process. The extent of information removal ultimately is uncertain because there is no official accounting for what information has been removed or was never posted because of security concerns.

Securing Scientific Research and Academic Institutions

Recently, attempts have been made to expand restrictions on the availability of sensitive information to scientific research and publication. As discussed above, concern has particularly focused on, but has not been limited to, the life sciences. The Union of Concerned Scientists alleges that the Bush administration "often imposes restrictions on what government scientists can say or write about 'sensitive' topics" and that the scope of the "manipulation, suppression, and misrepresentation . . . is unprecedented" (Union of Concerned Scientists 2002). For example, Dr. James Zahn, a USDA microbiologist conducting swine research, claims that the USDA's February 2002 policy for reviewing "sensitive issues" has placed "a chokehold on objective research" (Beeman 2002). He further claims that the USDA forces controversial research through an extended appeals process, prevents researchers from publishing their sensitive findings in scientific journals and at public meetings, and cooperates with industry groups to suppress findings that do not jibe with their interests.

Outside the realm of the life sciences and government-controlled research, Sean Gorman's research as a Ph.D. candidate at George Mason University helped underscore the dangers of aggregating infrastructure information in an academic setting. His dissertation, which maps the nation's fiber-optic infrastructure, provides vulnerability information that experts have labeled a "terrorist treasure map" (Blumenfeld 2003). Corporate CEOs have asked that Gorman's work be

[19] DOD Directives and Regulations—including those referenced in this paper—were present on the DOD website while this paper was being researched. They were removed for a short period, but they are available again.

classified even though there is no current legal basis for limiting access to such publicly available information.

Restrictions on Foreign Students and Researchers

The administration recently established the Interagency Panel on Advanced Science and Security (IPASS), which determines whether students applying to enter the US will study in fields that have direct relevance to weapons of mass destruction. Charles Vest, President of MIT, suggests that this approach to foreign student policy has both positive and negative aspects (Vest 2002). Vest argues that the framework has three positive features: it is based on a high-level review panel rather than a list of subjects or courses considered off-limits; it applies only to fields related to weapons of mass destruction; and restrictions are determined during the visa process so that openness of academic institutions can be maximized. He also sees three situations where IPASS would disrupt the normal workings of universities: moving beyond the criteria that are based narrowly on weapons of mass destruction; expanding criteria to cover academic courses rather than very specific research; and applying new academic restrictions to students after they have begun study with a proper visa.

In addition to the IPASS process, a Mantis[20] investigation by relevant agencies is triggered if a visa seeker mentions a key term in a database (Department of State 2002). Like Mantis, the Student and Exchange Visitor Information System (SEVIS) began before September 11, 2001. SEVIS is designed to be a real-time system for tracking the movements of nearly five hundred thousand foreign students, scholars, and scientists in the United States (United States Embassy in Seoul 2003). Additionally, the new Visa Condor system flags "nationals of certain countries of concern," again triggering an investigation (Boucher 2002).[21] All of these checks slow the process of obtaining visas even though most of them were intended to impose no more than thirty-day delays.

Restrictions on foreign students imposed by the Illegal Immigration Reform and Responsibilities Act of 1996 are now being enforced in full and the Patriot Act expanded these controls. The State Department's Technology Alert List (TAL) (Department of State 2000) has been updated to reflect "major fields of

[20] The Visa Mantis program is designed to serve four security objectives. Specifically, its objectives are to stem the proliferation of weapons of mass destruction and missile delivery systems, restrain the development of destabilizing conventional military capabilities in certain regions of the world, prevent the transfer of arms and sensitive dual-use items to terrorist states, and maintain U.S. advantages in certain "militarily critical" technologies. An Eagle Mantis clearance is a no-response check that allows posts to conclude their investigations after a ten-day wait. A Donkey Mantis clearance requires the State Department's authorization before the case is processed to its conclusion.

[21] Posts abroad submit names to the Visa Condor program, triggering further analysis by the appropriate U.S. agencies. This process is supposed to take no more than thirty days.

technology transfer concern" (Using the Technology Alert List: Update 2002). Tab A of the update provides detailed descriptions and examples of each area identified on the Critical Field List (CFL) on the TAL. Of obvious concern is that the CFL as enumerated in the TAL may be too broad to do any good. Alternatively, the specifics in the update may lead State Department officials to construe restrictions too narrowly. State Department officials reviewing visa applications are urged to refer to the TAL and consult with their superiors, while also trusting their "BCISTINCTS [*sic*, meaning 'basic instincts']" (Using the Technology Alert List: Update 2002). On the whole, the approach of defining broad categories tied to focused examples while leaving room for subjective human judgments seems like a good fit.

It is hard to separate the effects of the visa policies from the worldwide economic downturn—both of which could contribute to the diminishing visa application growth rate.[22] Despite a number of horror stories that have received heavy media coverage, it is believed that the vast majority of foreign students that apply are making their way into—or back into—the United States. However, problems clearly remain. *The Washington Post* publicized at least three such horror stories—"What Does a Scientist Have to Do With Terrorism?" (Jordan 2003); "A Scholar Confronts 'Ugly Face of America' (Brown 2003); and "Post-9/11 Visa Rules Keep Thousands From Coming to U.S." (Hockstader 2003)—in only two days in mid-November 2003. Overall, to date, it is difficult to measure the full impact of the visa policies because it is not clear who the policies are deterring from applying. Although there has been a measurable drop-off in applications from specific countries, such as Iran and Iraq, they have been compensated for by increases from other countries. If foreign students perceive the policies to be too widely targeted or if they object to potentially undergoing additional checks beyond their face-to-face consular interview, then they may attend educational institutions in other countries, and such a shift already has been perceived. It is hard to say that such a policy is effectively asserting the security interests of the United States.

On the whole, the new policies have introduced an additional level of uncertainty into the process. However, the most current data indicate that a majority of foreign students are having success entering U.S. institutions—nonetheless, this may be a lagging indicator because student planning lead-time could be in years. Additionally, while the *growth rate* of the number of students applying to study in the United States has fallen, it has not dropped to or below zero—correspondingly, the *actual number* of foreign students in the United States has increased (Institute of International Education – Open Doors 2003 2003).[23] It will be interesting to see if and how the numbers change as more studies are con-

[22] The rate has nearly leveled off, though it is still growing.

[23] Although it is unlikely, an alternate explanation for the drop in the growth rate is that U.S. educational institutions are nearing their saturation points.

ducted and more data becomes available, post-implementation.

The Homeland Security Act of 2002 and Current Protection of Sensitive Information

The Homeland Security Act of 2002 establishes two new designations for the control of information—namely, sensitive homeland security information (SHSI) and critical infrastructure information (CII). SHSI encapsulates information originating in and shared between federal, state, and local government. CII refers to information originating in the private sector that companies voluntarily disclose to the government for safeguarding.

Sensitive Homeland Security Information

The policy on sensitive homeland security information has not been spelled out clearly or completely. However, sections 891 through 893 of the Homeland Security Act do provide a high-level description of SHSI. Specifically, it is any information that:

- Relates to the threat of terrorist activity;
- Relates to the ability to prevent, interdict, or disrupt terrorist activity;
- Would improve the identification of suspected terrorists; or
- Would improve the response to a terrorist act.

The Card memorandum mentioned above tasked OMB with defining SHSI. However, section 893 of the legislation shifted this responsibility to the president himself. The president, in turn, delegated responsibility to the Department of Homeland Security (President 2003b), though the report still was due no later than November 2003—one year after the passage of the Homeland Security Act.[24]

These sections of the Homeland Security Act also begin to establish protocols for sharing sensitive information between federal, state, and local agencies. Information given to the federal government is exempt from any state and local laws that may require the disclosure of said information. Public officials may

[24] Steven Aftergood of the Federation of American Scientists submitted an FOIA request for "a copy of the Non-Disclosure Agreement that is required by the Department of Homeland Security as a condition for sharing of sensitive information . . ." (Withnell 2004). In response to the request, DHS stated that they are "currently working to develop procedures for the sharing of sensitive homeland security information. At this time, however, these procedures have not been finalized."

receive SHSI if they either have been granted a security clearance or have entered into non-disclosure agreements with the appropriate federal agencies. However, because it is unfeasible to process security clearances for all of the people who would need access to such information, information sharing typically has proceeded via rapidly-administered non-disclosure agreements.[25]

Critical Infrastructure Information

Critical Infrastructure Information, as established in section 214 of the Homeland Security Act, covers information voluntarily submitted to a federal agency for "analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes." CII is exempted from public disclosure under FOIA,[26] and it cannot be used directly by an agency in any civil action—federal or state—if such information is submitted in good faith. Submitting information under the rubric of CII does not waive one's right to privilege or protection, such as patent or copyright. Many people fear that corporations will use the protections of CII to reveal dangerous practices, such as polluting activities, in order to insulate themselves from prosecution and to prevent these secrets from ever becoming public knowledge. However, CII does not cover information that would otherwise be discovered "lawfully and properly." Therefore, if the government or private citizens would come into contact with such information in other ways—for example, tracing pollution in a stream to its source—then the polluting company would not be guaranteed protection. Again, it is not feasible to grant security clearances to all of the public servants who would need to come into contact with CII. The concern is not one-sided—private sector companies worry that turning information over to the government may lead to new and/or additional requirements for the costly protection of infrastructure (Mintz 2004).

Putting the Pieces Together

The definition of SHSI is, to date, incomplete, and the potential exploitation of CII—for example, publishing the critical nodes in the telecommunications

[25] In addition to the resource requirements associated with conducting an investigation to grant a security clearance, the situation might be moot by the time the clearance is granted.

[26] CII ordinarily would be protected by exemption category 4, which covers "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." However, the Homeland Security Act gave CII greater protection by specifically exempting it from disclosure within the law. This implies that CII should be protected from disclosure under the more robust FOIA exemption category 3, which protects information "specifically exempted from disclosure by statute."

network—frequently raises serious security concerns. Perhaps more important than problems with either of the two designations is the seeming lack of coordination between the two policies. Additionally, the Homeland Security Act does not address the issues raised by academic/scientific information. If the goal of the policies set forth in the Homeland Security Act is to control sensitive homeland security information, then it follows that some controls must be put on academic/scientific information.

SHSI and CII, although a step in the right direction, are an imperfect start. A system for maintaining controlled unclassified security information (CUSI) would unify these current measures and account for sensitive information arising in the academic/scientific sector. More importantly, CUSI would create a coherent and complete policy definition, coordinating implementation efforts across all sectors of society. A CUSI regime then becomes a way of safeguarding information that, if improperly disseminated and utilized, could egregiously endanger public safety. This new policy for controlling information must be carefully engineered to address the inevitable legal and process challenges posed by the First and Fifth Amendments, maintaining a default tendency toward openness.

Section II: Toward a Framework for Information Security Policy

Underlying Policy Questions

There are four key questions that underlie the crafting of an information security policy. First, how do you define and identify security-related information that should be controlled? In order to have an effective control regime, it is essential to have a clear vision of what information should be controlled. This question addresses the "what" of the policy. Second, who should control homeland security information? There may be government control, private control, or some public-private partnership for managing the information. This question addresses the "who" aspect of the policy. Third, to what extent should homeland security information be controlled? Depending on the setting in which the information arises, this "how" question asks whether and to what degree there should be government regulation vis-à-vis other forms of regulation. Finally, how do you balance security with openness? There is a clear desire for greater security in the post-September 11 order. However, security must be maintained in a way compatible with the broader values that comprise our notion of freedom as well as the scientific benefits of open exchange of knowledge. Taken as a whole, then, the answers to these questions constitute the definition of a good policy for information security that is mindful of the benefits of openness.

Policy Objective and Definition of Controlled Unclassified Security Information

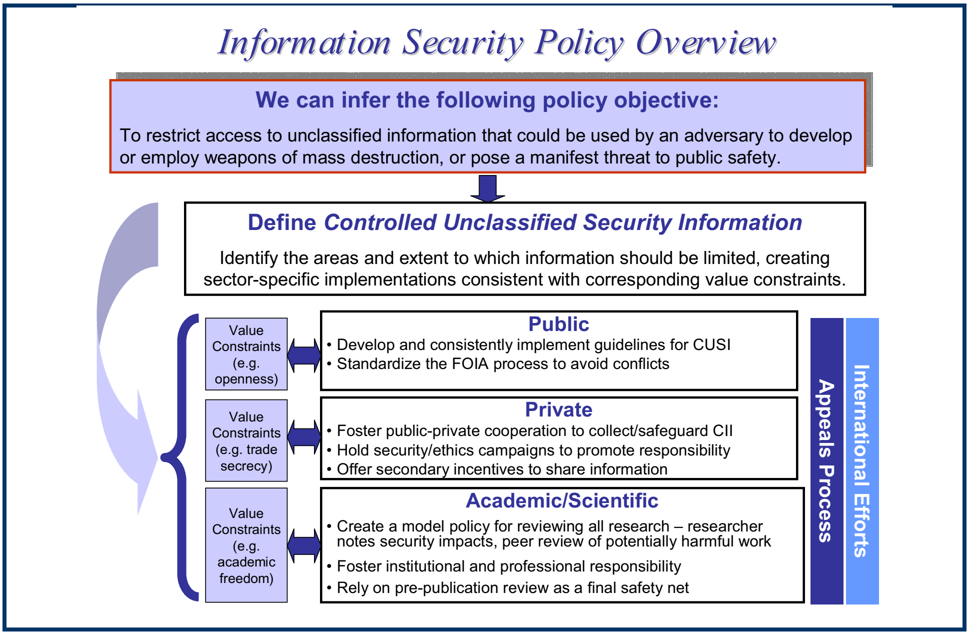
Understanding the policy objective and forming a definition of controlled unclassified security information begins to phrase the answers to the questions posed above. While not explicitly stated, there is a desire for an overarching policy objective and a definition of "sensitive information" that applies to all three sectors—public, private, and academic/scientific (see Figure 1). The government's policy objective can be understood as moving from this broad desire to comprehensively limit access to sensitive, unclassified information, to the more focused goal of ensuring security by restricting access to unclassified information that could be used by an adversary, adversarial group, or nation to develop or employ weapons of mass destruction, or pose a manifest threat to public safety.

Areas of sensitive information should be identified and assessed, independent of sector. Regardless of where sensitive information originates, it is still sensitive. However, the values that constrain regulation are particular to each sector. Linking the implementation to the sector-specific values—including openness, autonomy, and academic freedom—allows for finely-tuned, appropriate implementations. While the definition of what information is sensitive remains constant and implies a need for controls, the same controls are not appropriate in all sectors. Therefore, determining where the information originates and resides affects the control options available to the government. Education campaigns, an appeals process, and international efforts span all three sectors.

Spheres of Impact

Value Constraints in the Public, Private, and Academic/Scientific Sectors

The particularities endemic to the public, private, or academic/scientific domains in which sensitive information is produced complicate the crafting of a single governing policy. For example, a policy governing the results of a university study might not be appropriate for sensitive information produced by the intelligence community. Moreover, certain values stand out among each sector. These values constrain the ways a policy can be implemented. Salient value constraints include the openness and responsiveness of the public sector, a respect for trade secrecy and autonomy in the private sector, and collaboration and deference to academic freedom within the academic/scientific sector.



Information Security Policy Overview

We can infer the following policy objective:

To restrict access to unclassified information that could be used by an adversary to develop or employ weapons of mass destruction, or pose a manifest threat to public safety.

Define *Controlled Unclassified Security Information*

Identify the areas and extent to which information should be limited, creating sector-specific implementations consistent with corresponding value constraints.

Value Constraints (e.g. openness)

Public
- Develop and consistently implement guidelines for CUSI
- Standardize the FOIA process to avoid conflicts

Value Constraints (e.g. trade secrecy)

Private
- Foster public-private cooperation to collect/safeguard CII
- Hold security/ethics campaigns to promote responsibility
- Offer secondary incentives to share information

Value Constraints (e.g. academic freedom)

Academic/Scientific
- Create a model policy for reviewing all research – researcher notes security impacts, peer review of potentially harmful work
- Foster institutional and professional responsibility
- Rely on pre-publication review as a final safety net

Appeals Process

International Efforts

Figure 1: Information Security Policy Overview

The Problem of Overlap

The public, private, and academic/scientific spheres are not necessarily mutually exclusive. Protecting sensitive information therefore becomes more difficult when considering companies or organizations that have a strong role in more than one sector. Private companies like the Lockheed Martin Corporation depend on contracts with the federal government. Similarly, the Institute for Genomic Research cooperates with the National Institutes of Health on a number of research projects. The breakdown into sectors does not completely resolve this problem of overlap (see Figure 2), but it does illustrate where conflicts arise and provide a mechanism for resolving ambiguity by making explicit the particular value constraints and implementation options.

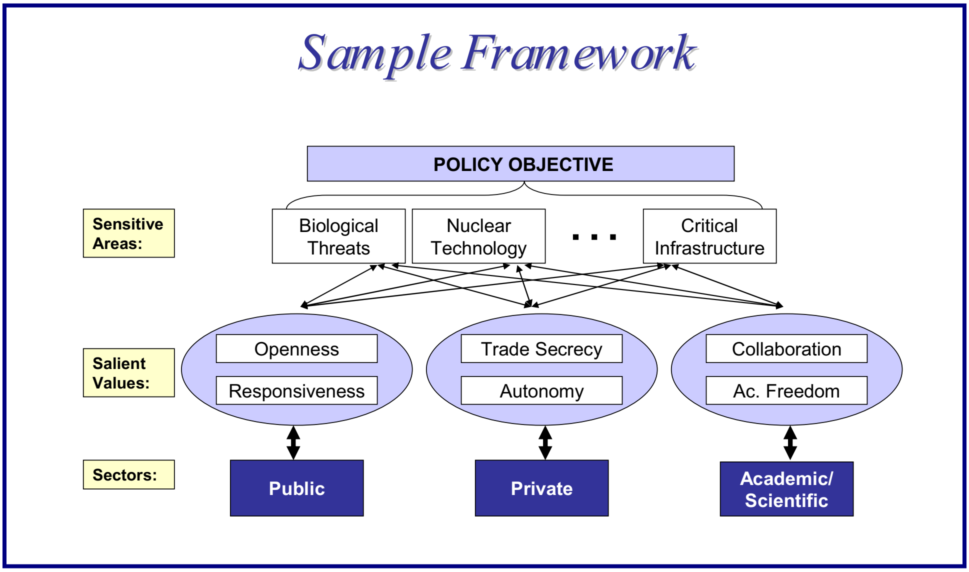


Figure 2: Sample Framework, Illustrating the Problem of Overlap

Section III: Proposal for Controlled Unclassified Security Information

Defining CUSI

The first step in consolidating, coordinating, and refining existing policies aimed at protecting unclassified, sensitive information is to develop a clear understanding of what and how security information should be identified and controlled. We propose a system for maintaining *controlled unclassified security information* (CUSI). It is, however, extremely difficult to identify CUSI *prima facie*. The principle of "I'll know it when I see it" generally applies to CUSI materials, but an *ex post* designation may be too late to do any good. The 1994 Joint Security Commission Report "Redefining Security" illustrates the broad range of information—apart from information relating to weapons of mass destruction—that might be considered Sensitive but Unclassified (SBU):

> We have in mind information about, and contained in, our air traffic control system, the social security system, the banking, credit, and stock market systems, the telephone and communication networks, and the power grids and pipeline networks (Joint Security Commission 1994).

CUSI would consist of information that, if improperly disseminated and utilized, could egregiously endanger public safety. As such, it would be a unification of current measures—sensitive homeland security information (SHSI) and critical infrastructure information (CII)—while also identifying areas that academic/scientific institutions should carefully scrutinize. Unlike the piecemeal policies that are developing today, CUSI accounts for information arising in all three sectors, creating a coherent and complete policy. Moreover, it also coordinates implementation efforts across all sectors.

The president, in consultation with the Departments of Defense, Energy, Health and Human Services, Homeland Security, Justice, and other departments and agencies as appropriate should therefore create definitions for CUSI—including guidelines for access, dissemination, control, and release. These guidelines should address the following three areas of sensitive information, which are best understood through examples of their major constituent concerns:

Information relating to Weapons of Mass Destruction

Following in the spirit of the Card memorandum discussed above, most information—especially information that is government-controlled—relating to the research and development, production, and employment of weapons of mass destruction should be controlled in order to prevent this information from supporting any efforts of adversaries. It may be demanding to implement such a control regime, as the scope of information that could be useful for the development of weapons of mass destruction continues to expand because of dual-use fundamental technologies that enable, for example, chemical and biological weapons. Research and development refers to the beginning stages of creating a weapon of mass destruction. Restricting research and development must rely on constraining knowledge rather than forbidding it. For example, such restrictions would control research into the engineering of viral factors that introduce animal pathogens into humans but would not prohibit it, categorically. Production refers to the ways in which information can be weaponized, or leveraged against the public. As such, production restraints should entail issues similar to ways of refining anthrax and ways of enriching uranium. Although information about weapons programs would be classified, scientific "know-how" that may be—as in the case of bioweapons—only one step away from implementation generally would not be classified. Employment refers to final-stage delivery. For example, issues of employment may refer to detailed schematics on the briefcases used in the Tokyo sarin gas attacks or plans for maximizing the radiological contamination from a "dirty bomb."[27]

Critical Infrastructure Information

The United States has become extremely dependent on its critical infrastructure to deliver essential services—energy, banking and finance, transportation, telecommunications, and vital human services—that are critical to maintaining its national defense, public safety, economic prosperity, and a high quality of life. With so much critical infrastructure present throughout the United States, limiting information that could be used to threaten it seems especially daunting. Compounding the problem, much of this infrastructure has limited if any security at sites that would cripple segments of the country if destroyed. Therefore, restricting access to selected information seems exceedingly prudent. For example, specific information on site vulnerabilities should not be available except to those responsible for providing protection. Many of the critical nodes referenced in Gorman's Ph.D. thesis are unprotected, and disabling a limited number of them has the potential to impact telecommunications, banking, etc. at the national level. Similarly, information describing the exact geolocation of containment ar-

[27] The principal type of "dirty bomb," or Radiological Dispersal Device (RDD), combines a conventional explosive, such as dynamite, with radioactive material. The objective is not to create a nuclear explosion, but rather to contaminate an area with a radioactive isotope.

eas or physical vulnerabilities of nuclear power plants could provide guidelines for an attack.

A second category of infrastructure information that should be protected is contingency and recovery plans. Many aspects of contingency plans—including evacuation routes and shelter areas—need to be disseminated widely so that the public will be prepared to respond. Some aspects, such as response and communication plans, are only needed by and should only be made available to key leaders, planners, and those responsible for responding. Making this information broadly available enables terrorists to combine attacks to produce a much greater impact. For example, a terrorist could monitor the responder communications frequencies in order to plan additional attacks, disrupt recovery efforts, avoid detection, and escape pursuit.

Intelligence and Security Information

As discussed above, sensitive homeland security information (SHSI) as proposed in the Homeland Security Act consists of intelligence information that must be shared between federal, state, and local officials to prevent and react to terrorist attacks. The law provides two mechanisms for controlling access to such information—namely, issuing clearances or entering into non-disclosure agreements. However, it is not practical to issue security clearances in advance to all of the people who would need access to such information in order to respond to all possible contingencies. Moreover, needs may arise so quickly that it would be impossible to grant security clearances during or after the fact. Therefore, there must be a way of distilling classified information into "merely" sensitive information that is usable by authorities with quickly-administered non-disclosure agreements, while protecting the sources and methods used to collect it. For example, it may be sufficient for authorities to know that a certain type of attack is expected on a certain day. This protects the truly secret parts of the information, but enables non-cleared officials with a need-to-know to do their jobs.

A related category of information consists largely of rules, procedures, and specifications that should be protected because their release would jeopardize security efforts (Sollenberger 2004). A prime example is sensitive security information (SSI), now folded into Transportation Security Administration (TSA) policy as part of the Transportation Security Regulations.[28] SSI includes "information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment . . ." (Department of Transportation 2002). Building on the TSA example, if such

[28] 14 CFR 91, 107, 108, 109, 121, 129, 135, 139, and 191 described the existing FAA regulations, and their transference to the TSA is captured in 49 CFR 1500, 1520, 1540, 1544, 1546, 1548, and 1550.

information were readily available, it might be possible for terrorists to avoid detection by altering their travel patterns or by using electronic devices to interfere with screening equipment.

Guiding Criteria for Designating Material CUSI

Based on these three areas of concern, we propose a systematic method for governing the decision to designate material CUSI, geared around four guiding questions.[29] The answers to the questions that designators should ask are not always clear and unambiguous—accordingly, the default position should be to release information. Also, throughout the designation process, there is significant room for individual, thoughtful discretionary disclosure.

Would knowledge of the information help a terrorist threaten public safety?

In answering this question, one must not only consider the specific information, but also the "data map"—the broader context—in which the information exists. Pieces of information may be viewed as tiles in a mosaic. Once enough seemingly innocuous information is released and assembled, the whole picture may become clear. This greatly complicates the process of determining what information is truly sensitive (Strickland 2003). However, if knowledge of such information cannot be used by terrorists, then it should not be designated CUSI. Furthermore, if the answer to this question is not a clear and unambiguous "yes," then the information should not be controlled.

Is the information already available in the public domain?

Just because information is available in the public space is not in itself justification that it should remain—or its derivatives be made—available. For example, the information Gorman gathered and analyzed for his Ph.D. thesis was readily available. Clearly, a knowledgeable terrorist could have collected that information and performed a similar analysis. But widely distributing his paper provides a blueprint for attacking the critical communications network. Still, the burden should be placed on proving that information already available should be withheld. The grounds that are sufficient for establishing proof should be established *a priori* in accordance with the principles and guidelines that follow below.

[29] These questions in part are patterned after Aftergood and Kelly's guiding principles for determining what information should be considered SBU (Aftergood 2002).

If the information is currently available to the public, is there any reasonable way of controlling it?

Perhaps the most challenging part of crafting a good information security policy is determining when information that is already available in the public domain ought not to be. Trying to rein-in information that already has been widely disseminated may prove to be a daunting—or even impossible—task, especially when the information is already available and/or in use abroad. Government already has tried to retract or alter information that was once available online (Milbank 2003). As noted above, many departments and agencies have removed content from their sites. Rather than removing them completely, the Secret Service has opted to airbrush and blur aerial photographs of some key buildings in Washington, D.C. (Poulsen 2003). Although digital duplicates of the original photographs still exist online, they are now harder to find. Although restricting accessibility does not remove all traces of information, increasing the amount of work needed to find and utilize certain information may increase security.

If the information is not available in the public domain, are there any countervailing considerations that might militate in favor of disclosure?

There is some information that should be available for thorough public scrutiny. This includes information regarding environmental hazards, defective products, and risky corporate practices. Critics of the provisions of CII have focused on the ability of corporations to exploit the rules regarding exemption from civil suits. Unlike CII, the CUSI guidelines should provide an important check on private-sector corporations submitting information under the rubric of CII or CUSI with the intention of having it withheld from the public.

Not all documents containing the word "anthrax" pose security threats—information on how to produce weapons grade anthrax does,[30] information on its treatment does not, and information on its handling might. In this last case, security and openness may come into conflict. While there may be cases where it might seem more appropriate to err on the side of security rather than on openness, there are cases, such as this one, where the countervailing considerations of public health, medical research, and emergency planning militate in favor of disclosure.

While the media is not the message, it may matter whether information is available online, in print-form only, at designated reading-rooms, etc. Although it may be difficult to completely control information that is released to the public,

[30] Weapons grade anthrax would be pure and highly-refined, consisting of particles so fine that they can spread through air without detection.

security may be sufficiently served by limiting how and where the information is published. For example, emergency procedures relating to accident scenarios at nuclear facilities should be public knowledge to people who live within a close proximity, but there is no good reason why such information should be available nationally or internationally through the Internet. This question helps bring to light concerns about both dissemination and handling of sensitive information.

In the absence of any overriding public interest for the disclosure of the information, and because this information has already been deemed a threat to public safety, it should be withheld.

Recommendation: The president, in order to replace the piecemeal policies that currently are in place, should issue an executive order that identifies the types of information that should be designated CUSI, specify who has the authority to designate it, and create guidelines for access, dissemination, control, release, and penalties for violations.

The Key Elements of Information Security: Regulation, Cooperation, and Review

Government regulation, as a means of identifying and securing information, defines policies and procedures for controlling a well-defined set of information. Many such controls are currently in place. Classification policy is the primary tool for controlling information critical to the national security. Additionally, there are other forms of regulation that seek to control access to certain unclassified information. For example, information on individuals is protected from disclosure between federal agencies under the Privacy Act of 1974 (Department of Justice 2002b).

Stopping short of government regulation, self-enforcing mechanisms such as peer review and community responsibility provide a system that delegates responsibility to the members of a community or organization to identify and restrict the flow of their information. For example, physicists during World War II, realizing the destructive potential of nuclear research, instituted a self-imposed publication ban. The Advisory Committee on Scientific Publication was established to review all papers concerning uranium and other national security issues (The National Academies 2002). This system set up channels for scientists legitimately working in the field to have access to information, while keeping it out of the hands of Germany's scientists. And, in the fields of medical research, although so-called "bad science" can yield humanitarian results, researchers are loathe to pursue experimentation that their peers may consider unethical or otherwise unrepeatable—for example, scientists generally will not use the results from the Tuskegee experiments, where treatment was denied to syphilis patients over a thirty- year period.[31] As in these examples, rather than adopt a one-size-fits-all solution across sectors and types of information, the government must rely on a mixture of regulation, cooperation, and review for administering the CUSI system.

The Public Sector: Coordinating, Consolidating, and Sharing Information Generated and Controlled by the Government

There should be government-wide standards for determining whether certain information should be designated as CUSI, ensuring that similar information produced in different agencies is identified and protected in the same way.[32] These guidelines should, in turn, be implemented in all departments and agencies. CUSI originating in the Food and Drug Administration potentially is just as important as that arising from the Centers for Disease Control and Prevention and the Department of Homeland Security. Thus, the same protections must be guaranteed for similar CUSI materials originating in different agencies.

Along with these protective measures, the implementation of FOIA policy must be reviewed to ensure that it is consistently applied across all departments and agencies to provide for the appropriate protection of CUSI. This will ensure that the FOIA and CUSI guidelines do not come into conflict, or, more specifically, that an agency operating under FOIA rules does not violate the attendant CUSI rules.[33] Department and agency heads have not significantly increased their classification activity pursuant to the Ashcroft memorandum; however, the language reminds classification authorities of their responsibilities to the broader public safety. As such, the Ashcroft memorandum becomes an important symbol for sensitizing public officials. The administration should also encourage consul-

[31] Current American Medical Association Policy E-2.30 Information from Unethical Experiments states: "Based on both scientific and moral grounds, data obtained from cruel and inhumane experiments, such as data collected from the Nazi experiments and data collected from the Tuskegee Study, should virtually never be published or cited. In the extremely rare case when no other data exist and human lives would certainly be lost without the knowledge obtained from use of such data, publication or citation is permissible. In such a case, the disclosure should cite the specific reasons and clearly justify the necessity for citation."

[32] Although some information from private corporations and federally-funded research may be controlled by the federal government, the ways in which these types of information are different from typical government-controlled information—e.g. their nature and the acceptable ways they can be controlled—require a longer, more detailed discussion that follows below.

[33] To this end, the laws defining CUSI should specifically exempt such information from disclosure, which therefore would protect CUSI from disclosure under FOIA exemption category 3.

tations with the FOIA Counselor Service[34] to ensure that departments and agencies are operating with the same set of disclosure rules. The FOIA Counselor Service should serve as a resource for reviewing difficult cases and providing education to departments and agencies. Formalizing the role of this "FOIA Hotline" would prevent issues of one agency releasing something when another agency refuses, as was the case with FOIA coversheets being withheld by DOD but released by the General Services Administration (Aftergood 2003). CUSI and FOIA should not be viewed as competing paradigms of protection; rather, with these minimal checks in place, CUSI and FOIA rules should work in concert to protect truly sensitive information.

Recommendation: Government departments and agencies should consistently implement a single, presidentially-defined government-wide policy for Controlled Unclassified Security Information (CUSI), and it should enable the sharing of sensitive materials between departments and agencies at the federal, state, and local levels, as well as with those in the private sector with a need-to-know.

The Private Sector: Sharing Information, Analyzing Interdependencies, and Mitigating Vulnerabilities

As discussed above, the current CII provisions established in the Homeland Security Act are designed to protect private information relating to infrastructure information that is transferred to the government. Indeed, the government should identify, issue guidelines for the protection of, and, in some cases, collect sensitive private information in order to conduct analyses of interdependencies and identify system level vulnerabilities so that they can be mitigated. By collecting information from a number of sources, government is in a unique position to identify interdependencies within and across critical infrastructure sectors, raising their awareness of where deeper vulnerabilities may lie.

The idea behind the current CII provisions is that protecting information under a more narrowly interpreted FOIA exemption will provide corporations with incentives to share information. However, the laws are structured more as guarantees—namely, the guaranteed exemption from civil suit—rather than incen-

[34] Through the FOIA Counselor Service, also dubbed the "FOIA Hotline," experienced FOIA attorneys provide information, advice, and assistance to personnel throughout federal departments and agencies, as well as other individuals with questions of interpretation and implementation. Occasionally, a more thorough consultation is needed in order to arrive at a final resolution, and, in these cases, agency representatives meet with the Department of Justice's Office of Information and Privacy (OIP) attorneys. OIP handled three thousand total cases in 2002, about three hundred fifty of which required the involvement of supervisory personnel and fifty-four of which required full consultations (Department of Justice 2003).

tives. A recent study has concluded that private firms, in the absence of appropriate incentives, will attempt to free ride—that is, they will attempt to benefit from other firms sharing security information without necessarily sharing their own (Gordon 2003). Although the provisions of CII intend to reveal vulnerability information to the government, the public has been concerned that the language is sufficiently vague, thus enabling private corporations to use the CII provisions to conceal harmful, illegal, or unethical practices. The language of the law should be changed to protect disclosure except where there is an overriding public interest.[35]

It may be more effective to educate corporations via security and ethics campaigns in addition to offering secondary incentives, such as subsidized insurance and guarantees that information will not be publicly disclosed or used in civil suit if it is submitted in good faith and there is not an overriding public interest. Such campaigns would avoid heavy-handed government regulation and interference, while eliciting a sector-wide corporate culture of thinking through security implications while encouraging the sharing of data with government. In addition to sensitizing corporations regarding security concerns, such campaigns would also lay the groundwork for a liability system that encourages self-regulation, whereby corporations are penalized through civil suit, loss of government contracts, or possible government-imposed financial sanctions for failing to comply with federal guidelines by attempting to conceal data inappropriately or failing to turn over sensitive information to the government when there is an overriding security interest.

Recommendation: The Department of Homeland Security's Directorate of Information Analysis and Infrastructure Protection should collect and protect sensitive private-sector information and craft an incentive structure to encourage private firms to share such data.

Academic/Scientific Sector: Encouraging Constrained Research and Publication

For academic and scientific research, a review process must be established so that it works at two stages—at the beginning of basic research into sensitive areas, and at the publication stage of sensitive research. We advocate a system that encourages researchers to think about the potential security implications upfront, establishing a peer review process for screening sensitive research, while publishers acting together with reviewers catch the harmful, often unintended results

[35] As discussed above, the CII protections have the potential to be abused because the definition of CII may be overly broad. The compromise of exemption from civil suit for "good faith" submissions leaves considerable room for ambiguity.

at the pre-publication phase.

Regardless of when the reviews take place, there are still concerns that scientists and academicians—whose jobs are normally to conduct their own, and adjudicate the merit of others', research—are not the right people to make security assessments. Similarly, security experts may not be able to comprehend the full implications of cutting-edge research. We argue, however, that it may be more efficient to educate and guide scientists and academicians to identify and reason about security concerns than to train security experts to become specialists in all fields of advanced research.

To this end*,* *all* researchers should become educated in security risks associated with their areas of research. There is a broad range of cases, extending from the creation of roadmaps like Gorman's Ph.D. thesis on infrastructure vulnerabilities, to the proper handling of dangerous pathogens like Butler's mismanagement of plague bacteria at Texas Tech University (Connolly 2003). Government should disseminate this information through workshops, communications with professional associations, and through collegial interactions. Researchers therefore would be in a better position to make determinations about their works' sensitivity.

While most recognize the real and growing danger that the misuse of science may pose, there are some—including Robert Rich, President of the Federation of American Societies for Experimental Biology—who are concerned that imposed restrictions will fail and that even weak, self-imposed restrictions may do more harm than good (Broad 2002). The alarm about terrorism and overreaction to the potential dangers of some scientific work may induce policy makers to impose security measures on research and publication that would be highly detrimental to the advancement of science and have insignificant, or even detrimental, national security impact.

Recommendation: DHS, in conjunction with other federal departments and with support from the NSF, should create and run education and awareness campaigns for both researchers and publishers that foster a spirit of institutional and professional responsibility to curb research into and publication of imminently dangerous information.

Guidelines for Federally-funded Researchers

We advocate establishing a system that encourages researchers to think about and disclose their potential security implications in self-assessments to an approval-granting authority, and having that work identified as having security implications, in turn screened by a peer-review process. Requiring *all* proposed research to undergo an upfront investigation is not possible or necessarily desirable. For government-funded research, the government may require additional reviews throughout the life of the research as a condition of the grant, although extreme measures are likely to be met with resistance.[36] We propose a less invasive policy that begins with requiring researchers to perform a self-evaluation and indicate whether or not their research has potential security implications and, if so, to identify them. To this end, scientists and academicians should evaluate their research on the basis of its potential effects, such as the weaponization of sensitive information and the development of WMD, threats to—or exposed vulnerabilities of—critical infrastructure, and intelligence and security information protection and sharing. This system should be emulated by other scientists and academicians whose funding may come from other sources.

The system of thoughtfully identifying security implications should work particularly well because it saves time during the review, while inadequately identifying implications would jeopardize the researcher's credibility, perhaps limiting future funding possibilities. The approval-granting authority would then review the researcher's notes and certify that any security implications have been properly identified, thought through, and, where possible, mitigated. DHS should oversee the administration of the panels.

For that research identified as having a potentially significant negative impact on security, a peer-led proposal review process should be established to determine how best to resolve this conflict between science and security. This system should be modeled on the National Science Foundation's process for peer review of proposals. DHS should spearhead an effort to develop lists of sub-area experts from the ranks of leading scientists and academicians, providing those experts with a security awareness orientation. Ultimately, that list and the experts' services should be made available to government research organizations. Review criteria should be designed to help focus assessments on the potential outcomes of the proposed research and to anticipate its effects—both good and bad. Specifically, the following questions should be pursued by the researcher upfront as well as by the reviewers during the peer review process:

- What may be the benefits of the proposed activity to society?
- What are the potential dangers of pursuing such research?
- Is there specific reason to believe that deleterious outcomes could be leveraged easily against the public?
- Will the results be disseminated broadly or should they be controlled?

Questions of this sort explicitly address security concerns; also, by assessing

[36] For example, there was considerable backlash relating to the DOD's proposed "Mandatory Procedures for Research and Technology Protection within the DOD," which would have regulated DOD-funded classified and unclassified work. Additionally, many universities do not accept any federal funding if there are any restrictions put in place.

the benefits of the proposed activity to society, reviewers also should anticipate the potential dangers, thus making the tradeoffs between potential security concerns and real advances more explicit. This process would create a class of constrained rather than forbidden knowledge, implying that controlling research conducted into sensitive areas translates into an immediate improvement in security in a minimally-intrusive way.

While there is danger that any "chilling effect" on research ultimately would be detrimental in the long-term for a number of reasons—including foregone advances and decreased security—the potential threat of emerging work in the sciences merits this minimally intrusive level of oversight. Moreover, these procedures are not significantly different from the increased scrutiny received by research consisting of "more than minimal risk," including most research that involves human subjects. Researchers also may be more willing to submit to such a procedure because the responsibility for review and approval would fall within their community of peers.

Guidelines for Non-federally-funded Researchers

Only 26 percent of all research and development expenditures were funded by the federal government, compared to 69 percent funded by private industry in 2001 (National Science Board 2002). Unfortunately, without a significant change in law, privately-funded and unfunded research may not be subjected to the same scrutiny as the federally-funded research. However, the above steps to sensitize researchers and train them to think about security implications should still be encouraged, and may even be accepted voluntarily. Indeed, non-government-funded researchers using recombinant DNA often subject their work to the NIH standards and voluntarily seek approval from government-controlled boards (Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology 2003), and, so long as this new government-sponsored review panel functions effectively and efficaciously, it is not unreasonable to expect some researchers to voluntarily disclose their security concerns and submit to government-led reviews.

Nevertheless, complete and uniform cooperation cannot reasonably be expected. DHS—assisted by the NSF, the NIH, and other federal departments and agencies—should develop a model policy for reviewing research with potential security implications so that non-federally-funded institutions can develop review processes outside of government. Further, DHS and the appropriate agencies should certify that the privately-run panels are adhering to the government-specified model guidelines.

It is still wise to foster a sense of responsibility and community obligation among scientists in order to have them self- and peer-regulate, while utilizing publishers for additional controls further along in the research process. The goal for both government-funded and privately-funded research is to create a culture that frowns on the research, experimentation, and publication of CUSI, much like the culture that constrains certain experimental techniques, such as stem-cell research, and restrains others, such as human cloning.

Recommendation: Federally-funded researchers should disclose potential security concerns in their grant proposals. DHS-monitored review panels will assess the security implications of the work with potentially significant negative impact in accordance with well-established guidelines.

Recommendation: DHS should lead the effort to develop model review policies, encouraging their adoption for non-federally-funded research and submission to the government-monitored review panel or an independent, government-certified review panel.

Guidelines for Publishers

Self-censorship at the point of publication has already gained preference among some bioscience publishers. In February 2003, following a meeting at the National Academies of Sciences to generate a dialogue between the security and bioscience communities, a number of bioscience journals agreed to a policy of self-censorship (Statement of Scientific Publication and Security 2003). According to this system, journal editors agreed to consider whether the potential risk of publishing articles might outweigh the scientific gain. In the first year, the American Society of Microbiology (ASM) flagged two out of fourteen thousand articles as unsuitable for publication, and both of these papers were likely to be published after changes were made (Harmon 2003). *Science* and other major journals also have adopted new policies of self-censorship (2003 Information for Contributors 2003).[37]

While the above process for researchers is primarily intended to constrain potentially harmful investigation, these guidelines also limit the dissemination of unintentionally produced, easily weaponized, or otherwise potentially harmful information that might arise due to the impossibility of anticipating all potential outcomes of research. Again, pre-publication editors and reviewers should participate in an education campaign to become sensitized to the issues described above. Once suitably educated, publishers, professional societies, and research institutes should assess research prior to publication by including security concerns in their pre-publication reviews. The same set of questions asked by the government-review panel should be asked by the pre-publication reviewers. Because this is such a decentralized process, a government-sponsored team should periodically evaluate the pre-publication reviewers to verify that standards are

[37] For example, *Science* indicates that if papers present “security concerns,” *Science* will solicit “advice from outside reviewers who have special knowledge and experience in that area.”

implemented consistently across different publications and disciplines, and that the government-defined guidelines are successfully restraining the publication of imminently dangerous information.

Finally, publishers should implement a two-tiered publication scheme for information that is valuable to a broader audience but still should be protected. They should publish high-level, low-fidelity descriptions in journals while reserving detailed content to controlled premium online access. This procedure enables general research to be available to an unrestricted audience, while allowing those who truly need access to specific details to be able to obtain them. Detailed background checks are not necessarily required—rather, publishers should make their premium content available at the institution level. A university, research organization, or medical institute could, in turn, take responsibility for determining who has access to the restricted information. For example, the ASM might provide limited journal access to a university's biochemistry department, which might certify the credentials of its students, staff, and faculty. This scheme shifts the responsibility for controlling the flow of information from the government to those entities that produce and disseminate the information as well as the institutions that use it. Of course, for government-funded research, the government may reserve the right to withhold all or part of the research, or decide where to publish it as a condition of the grant.

Recommendation: Government should train publishers to conduct reviews just before research is made available to serve as a safety net after research is already completed, and publishers should implement a two-tiered publication scheme to restrict detailed content to premium access where the credentials of the readers can be verified.

Overarching Elements

With the rules for each implementing policy in each sector in place, it is important to step back and address three areas that cut across these sector-specific guidelines—namely, educational campaigns, an appeals process, and the pursuit of international regulation. While educational campaigns should be tailored to the sector, the management of the appeals process and the pursuit of international regulation should be exclusively governmental undertakings.

Handling CUSI-designated Materials

The CUSI designation indicates material that warrants a degree of protection but does not fit within the framework of the national security classification system. Specific control measures should be adopted throughout all government departments and agencies. The implementing regulations must address access, safeguarding and storage, dissemination and transmission, destruction, and release of CUSI-designated materials.

Access addresses who may view CUSI-designated materials and where they may be viewed—for example, in a locked or windowless office, a specified reading-room, etc. Safeguarding and storage as well as dissemination and transmission procedures must limit the potential for unauthorized disclosure. The implementing regulation must specify proper labeling—possibly including stamps and coversheets—in order to indicate that the information is designated CUSI. Safeguarding and storage procedures must also specify whether CUSI materials may be left in the open or if they must be locked in offices or special containers. Unauthorized disclosure of CUSI materials may result in criminal and/or civil penalties, and government supervisors may take disciplinary action where appropriate, as described in the regulation.

Dissemination and transmission must address who may circulate CUSI materials and how they are circulated—for example, if first class, certified mail, or special carrier is required, and if an inner label must indicate that the contents are CUSI. Similarly, regulations must address whether CUSI is suitable for export and/or is accessible to foreign nationals. CUSI materials may need to be destroyed through shredding or burning. The implementing regulation must specify if there is a mandatory release deadline, a periodic re-designation process, and the process for release through the appeals process.

Educational Campaigns

The Under Secretary of Information Analysis and Infrastructure Protection in the Department of Homeland Security should lead the effort to educate key personnel—including journal editors, review staff, security officers, researchers, etc.—with the concept, rules, and guidelines of CUSI. Specifically, the workshops should have three objectives: to publicize sector-specific guidelines, to raise general awareness of security concerns, and to educate people so that they can measure the "work-factor"—that is, a metric for measuring the costs of obtaining and the convenience of using specific information—for leveraging potentially harmful information.

Objective 1: Sector-specific Guidelines

For the public sector, the workshops should clarify the government-policies to federal employees and remind them of the specific resources they can tap through federal departments and agencies. The private sector should be acquainted with the ethical and security reporting standards while also teaching employees to be forthcoming when disclosing information regarding critical points in the infrastructure and work that could relate to weapons of mass destruction. Federally-funded academicians and researchers should be familiarized with the CUSI-specific review procedures, while non-federally-funded academicians and researchers should be encouraged to adopt the government-sponsored model review policies. Publishers should continue their dialogs, though they should shift the discourse from negatively-construed censorship to positive-sounding professional responsibility. The workshops should include case studies that illustrate how rules and norms have been changed, including Professor Butler's mismanagement of the plague bacteria and his failure to comply with the federal select agents regulations.

Objective 2: Raising Awareness

Seemingly benign information can be used easily to endanger the national security, and this perverse dual-use is not always apparent. Accordingly, a series of case studies should help raise awareness of the potential dangers of the application of certain types of information. An important part of assessing security implications includes forecasting unintended results—both positive and negative—of research. A final aspect of awareness is familiarizing people with the resources that are available for help and/or guidance regarding CUSI policy guidelines and interpretation. These case studies should include a discussion of the threats posed by the misapplication of the information collected in Gorman's Ph.D. thesis on infrastructure vulnerabilities and then describe the guidance and worries the corporate community provided and conveyed. Also, these case studies should include the Institute for Biological Energy Alternatives' new virus-synthesis techniques, which could revolutionize the way vectors are created as well as the way bioterrorists "reload" their bioweapons.

Objective 3: The "Work-Factor" for Leveraging Dangerous Information

Although it often is difficult to tell what information produced by fundamental research could be used for harm, and protecting infrastructure seems almost impossible with the many points of vulnerability, government employees, private sector employees in selected areas, academicians, researchers, and publishers should be capable of broad-based judgments assessing the costs and challenges of leveraging information for use in endangering the public safety. When information that could threaten the public safety is easily accessible—that is, when the costs of obtaining it are low and the convenience of using it is relatively high—this "work-factor" for leveraging potentially harmful information provides a benchmark for determining whether information should be controlled. While high-level descriptions of and mitigations for vulnerabilities should be released to inform and alert the public, "push-button" or "cookbook" instructions on how to do harm are easily identifiable and clearly should be withheld. The amount of resources, including the number of knowledgeable personnel, needed to exploit vulnerabilities describes a work-factor, which is a good, practical indicator of where disclosure borders on weaponization. For example, determining a work-factor is useful for judging biological research despite the perceived small gap between pure research and its application, as it takes both resources and a minimum set of skills for terrorists to develop and employ biological weapons.

The following figures illustrate how the work-factor might be used to signal where and to what extent information should be controlled, by first decomposing potential threats into low, medium, and high potential impacts. The assessments of cost and convenience are then simplified into discrete categories. In some cases, it may be possible to quantify cost and convenience more precisely—for example, given that there is both an International Atomic Energy Agency (IAEA) controlled and a black-market price for highly enriched uranium (HEU), and the level of effort to design and produce a nuclear weapon is known, the costs can be calculated.

The different shadings represent different levels of concern—blocks that are black represent the most severe threats, and blocks that are white represent threats that warrant a lesser amount of concern. Additionally, in the middle of these two levels of concern are grey blocks—though these threats often are difficult to reason about because they are ill-defined, poorly understood, or still new and emerging.

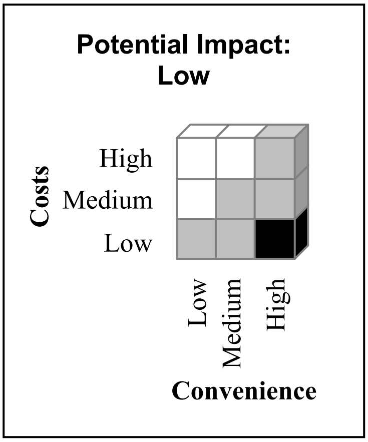


Figure 3: Levels of Concern for Low-Impact Events

For potential low-impact events, the most serious threats are those that are highly convenient and extremely low cost, as shown in Figure 3. Typically, these threats cause a high level of disruption and/or annoyance. An example of such a threat would be contaminating food with bacteria, similar to the 1984 case where members of a religious cult sprayed salmonella bacteria on salad bars throughout the Oregon region, causing 751 cases of food poisoning (Food Safety Department 2002).

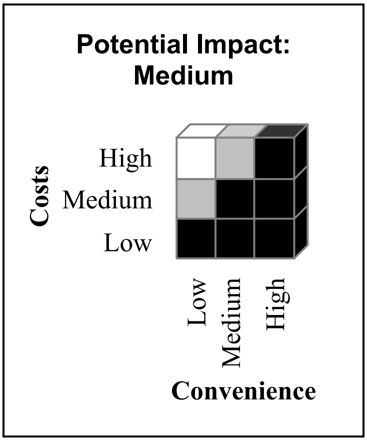


Figure 4: Levels of Concern for Medium-Impact Events

For a potential medium-impact event, those threats that are high in cost and low in convenience warrant the least amount of concern, as shown in Figure 4. Information on agents that when directly applied to fields would decrease crop yield without completely destroying the harvest might fall into this category. It would be difficult to deliver such agents, and decreasing the yield for some crops in the United States might succeed only in reducing the surplus.

Nearly all of the threats of a potential high-impact event should be considered serious, and information related to these threats should be controlled, as shown in Figure 5. A grey area, where information would have to be carefully evaluated, forms when costs are high and convenience is low. For example, information on how to create vaccines for highly-communicable diseases could fall into this category, as the method for creating vaccines now in use first increases the virulence of normal diseases and then finds inhibitors to block or antibodies to combat the strongest variants of the diseases. Increasing controls significantly could slow the development of preventive measures, which, in the end, might cause more harm than good.

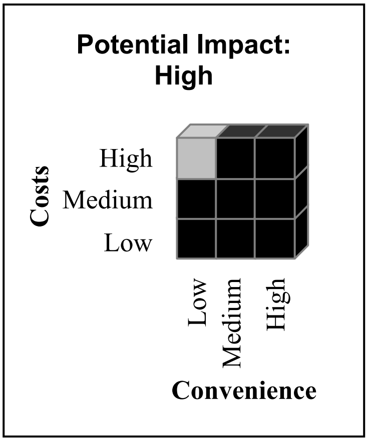


Figure 5: Levels of Concern for High-Impact Events

Recommendation: DHS should take proactive action to acquaint people with the concept of CUSI and sector-specific rules by completing a series of case studies, methodology developments, and workshops.

The Appeals Process

An appeals process allows individual decisions about the categorization of information to be reviewed on a case-by-case basis when deciding upon an initial designation as well as reviewing whether and to what extent already protected information should be redacted. An integral part of a regime for controlling sensitive information must provide a system for checking decisions on withholding information. One example of an established appeals process on which the CUSI appeals process might be patterned is the Interagency Security Classification Appeals Panel (ISCAP), established by Executive Order 12,958 in 1995 (President 2003a). Through this process individuals can appeal any agency's decision to keep information classified. From May 1996 through December 2002, ISCAP declassified significant portions of documents in 76 percent of all cases.[38] Specifically, 34 percent were fully disclosed and 42 percent were partially disclosed (Leonard 2003). However, ISCAP personnel currently may not be well-suited for undertaking the sorts of investigations necessary for making the most informed decisions about whether to terminate, withhold, or release unclassified, sensitive

[38] The ISOO's 2002 report to the president indicates that some of the data reported for FY2001 was incorrect, and these are the corrected numbers (Leonard 2003).

information.[39]

In order to promote legitimacy and ensure that the CUSI designation system is working, a two-level administrative appeals process should be established, as FOIA already provides a legal option. Such a process should have a clear vision and a mandate of bias towards openness. A senior appeals board overseeing a lower-level of review should ensure that reviewers have expertise on the information in question. Specifically, the higher-level appeals board should maintain an array of key people who own or are imminently connected to the information in question. The appropriate personnel could then come together and form ad hoc review teams. These teams should be capable of conducting thorough investigations that assess the potential impact of publishing or redacting specific details in relation to the data map more broadly conceived. The higher appeals panel—chaired by a senior DHS official and working in close consultation with the National Archives and Records Administration (NARA)—should have representatives from all sectors, and it should operate with the full confidence of the government, the public, and the academic and research community so that its rulings are seen as both legitimate and binding.

In addition to reviewing designations, the review process should address appeals from scientists who have their research limited upfront or at the prepublication phase. Even in this more judicial-based review scheme, reviewers should be able to undertake thorough investigations to assess the potential outcomes of conducting or releasing the research. Additionally, these reviews must be accomplished in a timely fashion—with response times mandated as part of the review.

Recommendation: DHS and NARA should administer an appeals process that has a clear vision and a mandate for openness, allowing for individual decisions about the categorization of information to be reviewed on a case-by-case basis, and in a timely fashion.

Pursuing International Regulation

International Regulation of Sensitive Information

Clearly not all scientific and academic information with obvious security implications originates domestically. Indeed, in 1999 the United States produced only about one-third of all scientific and technical papers. Therefore, there is an international dimension to the production and dissemination of sensitive informa-

[39] Working-level groups handle about 97 percent of all work and often make decisions, which the liaisons convey and approve, often without broader debate. ISCAP needs to function at a high-level to make binding decisions, give feedback, get input, and represent the agency and the agency's position.

tion, and simply controlling information domestically will not sufficiently limit all information that may be harmful. However, controlling sensitive information domestically—where the largest single-country percentage of all scientific and technical articles are produced—while operating with the confidence of policymakers, scientists, and the public, sets a standard for other countries. The spectrum for eliciting international control of sensitive information involves a comprehensive control regime (Brickley 2003) at one end, and a loose network of informal arrangements, particularly among publishers abroad, at the other.

One example of a comprehensive control regime is put forth by Dr. John Steinbruner of the University of Maryland's Center for International and Security Studies at Maryland. Steinbruner argues in favor of an international system to regulate research with dangerous pathogens, asserting that the peer review system is a useful but insufficient solution to the problem of controlling such research. His system would consider the security implications of research before it begins. An international body would monitor and legitimize all research that uses a select group of pathogens that are deemed most dangerous. This system has a tiered decision-making structure for balancing the dangers and openness of research. The most dangerous pathogens would be controlled at the international level, and this information would essentially be classified, though on a professional rather than national or supranational basis. At the local and national levels, less dangerous research would be regulated. Steinbruner's system is mandatory rather than voluntary, and it therefore would require significant international agreement to be implemented (Steinbruner 2003).

Before the administration takes proposals for limiting sensitive information abroad, however, we believe a working system must be implemented within the United States to establish the moral and practical ground for arguing that other nations should and can effectively alter their ways of conducting research and doing business. Once such a system exists within the United States and is operating with the confidence of policymakers, scientists, and the public, there are many channels through which foreign audiences can be reached—for example, through corresponding professional associations, ambassadors, etc. The United States along with Japan, Germany, and the United Kingdom account for approximately 60 percent of technical articles produced worldwide (National Science Board 2002), while OECD countries account for about 80 percent of the scientific and technical papers published worldwide (National Science Board 2002). An OECD-wide adoption of U.S. recommended policies could significantly limit the amount of sensitive information being spread freely.

Recommendation: Take proposals for international regulation of sensitive information abroad through all available channels after *the domestic system operates with the confidence of policymakers, scientists, and the public.*

Restrictions on Foreign Students and Researchers

Foreign students and researchers broadly contribute to many aspects of U.S. prosperity. Their most obvious contributions are to the development of the nation's intellectual capital. For example, having foreign students work in labs benefits both students and researchers, helping students gain experience and giving researchers quality labor. Limiting foreign students dries up the academic pool from which all students are drawn. Additionally, there are financial implications of limiting foreign students relating to lower enrollment and a loss of teaching assistants and professors. An American Institute of Physics report estimates that about 20 percent of foreign students initially were prevented from attending a U.S. university to enroll in a graduate physics program in 2003 (Neuschatz 2003). About 35 percent of all graduate degrees are conferred upon non-U.S. persons. Economists estimate that the United States earned $13 billion last year based on tuition fees, room and board, and other goods and services purchased by foreign students (Dobbs 2003).

Beyond these important intellectual and economic benefits, there is a broader, immeasurable societal impact, as foreign persons who remain in the United States after their studies are completed add value to our society through their cultural diversity. Even if foreign students return to their respective countries, connections are established abroad that expand the network of scientific collaboration and often serve as "good publicity" for the United States and its academic and scientific institutions.

According to the Institute of International Education (IIE) Open Doors study, the year-to-year growth rate of foreign students entering the United States has dropped from 6.4 percent two years ago to 0.6 percent over the last year. Although the number of students from Islamic states such as Saudi Arabia, Pakistan, and the United Arab Emirates dropped significantly, the decline was offset by major increases from India, South Korea, and Kenya (Institute of International Education – Open Doors 2003 2003). Visa restrictions seem to be the biggest reason for the slow-down in student enrollments and the delays in student registration. However, despite individual "horror stories" relating to long delays, IIE President Allan E. Goodman says that the United States is still "the number one destination for foreign students" and that most students were coming "without substantial delay" (Dobbs 2003). Indeed, the State Department and the U.S. Citizenship and Immigration Services (USCIS) have significantly reduced the time it takes to conduct their reviews (Jacobs 2003). Accordingly, they should publicize the successes most students have already had despite the purported strict regulations, while informing foreign students abroad who may be seeking to come to the United States that the new restrictions are not as bad as they are often portrayed. Additionally, the State Department and USCIS should communicate proactively with American universities to make sure that foreign students already studying in the United States become familiar with the updated regulations and comply with them to avoid any further hassles. Furthermore, because there are often lags between implementing changes and observing results, they should monitor the effects of the policies and adjust them based on this feedback.

Recommendation: The State Department and the U.S. Citizenship and Immigration Services (USCIS) should publicize and build on the successes most foreign students are having in the United States to continue to attract talented students while communicating the details of new programs and procedures to prospective and current students. Impacts from policy changes must be closely monitored and policies adjusted as feedback becomes observable.

Measures of Policy Performance

It is somewhat difficult to analyze the performance of the selected policy because of the many dimensions involved. We recommend a system of analysis that assesses the policy's performance in each of five categories, taking account of the differences between the public, private, and academic/scientific sectors. The first two metrics focus on miscues in the CUSI designation process, whereas the latter three focus on somewhat less tangible aspects of the CUSI policy.

1. <u>Information Security</u>: Information security relates primarily to Type I errors of CUSI designation—that is, this measure is designed to capture the extent to which information with security implications is released inappropriately. Type I errors may be very significant if the work-factor for leveraging the information is low.

2. <u>Information Openness</u>: Information openness refers primarily to Type II errors of CUSI designation—that is, openness should be measured by determining whether the CUSI designation is being used to withhold information inappropriately. Although it is tempting from a security perspective to say that these problems are not as important as Type I errors, Type II errors may be significant because they ultimately erode trust in the CUSI system and they may roadblock potentially beneficial avenues of research.
   Example: An effective way of measuring information security and information openness would be to assess the effectiveness of the prepublication review process by examining published and unpublished manuscripts from previous years to determine via *ex post* analysis how many articles should have been flagged as sensitive.

3. <u>Extent of Government Involvement</u>: Ultimately, government involvement should be minimized so that the CUSI designation system works

cleanly, quickly, and efficaciously. The CUSI system cannot work without real support from all three sectors, and, provided that all three sectors are making good-faith efforts to cooperate, excessive government involvement threatens the legitimacy of the policy.

4. <u>Research and Development Potential</u>: Research and development potential captures the ease with which academicians and scientists can openly and freely collaborate and publish. Also, it should capture whether researchers are avoiding specific areas because, for example, they believe their work will be preempted at either the pre-research or pre-publication phases.

5. <u>Feasibility of the Policy</u>: The feasibility of the policy is a qualitative measure that seeks to combine the willingness of agencies, corporations, and institutions to accept the policy, along with the practical challenges that enforcement must overcome. This approach to feasibility considers both constituent satisfaction of and confidence in CUSI policy.

Recommendation: The Directorate of Information Analysis and Infrastructure Protection of DHS should continuously evaluate the extent to which designating material CUSI increases security but leaves information accessible to those who need it, and it should continuously evaluate the review and appeals processes to ensure that standards are moving neither toward excessive secrecy nor imprudent openness.

Section IV: Summary of Recommendations

Policy Definition and Sector-specific Guidelines

Government must first develop a definition of controlled unclassified security information, identifying those areas that should be controlled regardless of the sector that produces such information. It also must recognize the value constraints that are particular to the public, private, and academic/scientific sectors. By doing so, government will be in a good position to identify the control mechanisms appropriate for each sector—including the specifics of *how* each mechanism should be implemented and *who* ought to implement them—taking into account the salient value constraints. Specifically, the public sector should adopt comprehensive, government-wide regulations. Government should rely on cooperative information-sharing programs with the private sector to obtain and safeguard their sensitive information. Finally, government should rely on timely, upfront reviews for the academic/scientific sector for government-funded research, while encouraging this process for non-government-funded research. These measures should be teamed with pre-publication reviews.

Overarching Elements: Education Campaigns, Appeal Process, and International Efforts

Apart from these sector-specific implementations, there are several overarching elements that apply to all sectors of society. First, the government should launch an education campaign to encourage cooperation, responsibility, and ethics to all producers of sensitive information. Second, government should establish a two-tiered appeals process with a clear vision and a mandate for openness. A first, low-level professional, administrative group should ensure that reviewers are connected to the information in question. The higher appeals panel should have representatives from all sectors, and it should have the full confidence of the research community, government, and the public. A flexible group of investigators should handle referrals from both levels, thoroughly understanding and analyzing the information in order to make educated decisions about the impacts of publications and redactions. The review process should also handle appeals from scientists who have their research limited.

Lastly, there is a clear international dimension to the control of sensitive information relating to both the information itself as well as the individuals who produce it. Once a domestic system for controlling sensitive information operates with the confidence of policymakers, scientists, and the public, there are many channels through which the governments can be reached. Foreign persons are critical to the success of the United States. The federal government should publicize the successes most students have had and inform foreign students abroad who may be seeking to come to the United States that the new restrictions are not as bad as they are often portrayed. The government, working with universities, should keep foreign students already in the United States updated so that they can comply with newer regulations in order to avoid any hassles, and these policies should be adjusted periodically based upon their effects, as they become observable.

Acknowledgments

The authors gratefully acknowledge research support from the Center for Technology and National Security Policy, National Defense University, through a grant with the Center for Public Policy and Private Enterprise, School of Public Policy, University of Maryland, College Park.

For the research above, and in many other areas of this report, the authors are greatly indebted to the assistance of Jonathan Roberts, who served as a Graduate Research Assistant at the Center for Public Policy and Private Enterprise.

The authors also gratefully acknowledge **Elisa Harris**, Research Fellow, Center for International and Security Studies at Maryland, Maryland School of Public Policy, University of Maryland, and **Lee Strickland**, Visiting Professor and Director, Center for Information Policy, College of Information Studies, University of Maryland, for comments on earlier drafts of this paper. Additionally, the following individuals provided invaluable insights during the course of this research:

Norma M. Allewell
Dean
College of Life Sciences
University of Maryland

William A. Arbaugh
Assistant Professor
Department of Computer Science
University of Maryland

Peggy DeBona
Assistant Director
Knight Center for Specialized Journalism
University of Maryland

Bruce W. Dearstyne
Interim Dean, College of Information Studies
University of Maryland

Howard Frank
Dean
Robert H. Smith School of Business
University of Maryland

Joseph JaJa
Director, UMIACS, and
Interim Director, Center for Bioinformatics and Computational Biology

Sam W. Joseph
Professor
Department of Cell Biology and Molecular Genetics
University of Maryland

Thomas Kunkel
Dean, Philip Merrill College of Journalism
University of Maryland, and
President and Publisher, American Journalism Review

Michael J. Kurtz
Assistant Archivist for Records Services
National Archives and Records Administration

Daniel J. Metcalfe
Director of Policy and Litigation
Office of Information and Privacy
Department of Justice

George Poste
CEO, Health Technology Networks, and
Director, Arizona Biodesign
Institute
Arizona State University

Rem Rieder
Editor and Senior Vice President
American Journalism Review

Thomas C. Schelling
Distinguished University Professor,
Department of Economics and
Maryland School of Public Policy
University of Maryland

John D. Steinbruner
Director
Center for International and Security
Studies at Maryland
University of Maryland

Robert S. Wachbroit
Research Scholar, Institute for Philosophy
and Public Policy, University of Maryland;
Adjunct Associate Professor of OB/GYN,
University of Maryland School of
Medicine; and Senior Research Fellow,
Kennedy Institute of Ethics, Georgetown
University

The authors also would like to thank **Steven Staats**, Graduate Research Assistant, Center for Public Policy and Private Enterprise, for research support.

Reference List

1. Terror in Tokyo. 1995. *The Economist* 334, no. 7907.
2. 2003 Information for Contributors. 2003. *Science* 299, no. 5603.
3. Statement of Scientific Publication and Security. 2003. *Science* 299, no. 5610.
4. "Invention Secrecy Activity, statistics reported by the U.S. Patent and Trademark Office, FY 1999-2003." Web page, [accessed 10 June 2004]. Available at http://www.fas.org/sgp/othergov/invention/stats.html.
5. Aftergood, Steven. 2003. Classified Info Cover Sheets Withheld, Released. *Secrecy News* Vol. 2003, no. 71.
6. Aftergood, Steven and Kelly Henry. 2002. Making Sense of Information Restrictions After September 11. *FAS Public Interest Report* Vol. 55, no. 2.
7. Albright, David. 1994. South Africa and the Affordable Bomb. *Bulletin of the Atomic Scientists* 50, no. 4.
8. Alexander, Arthur J. 1988. Soviet Weapons Acquisition in a period of New Economic Policies. Santa Monica, CA: Rand Corp.
9. Allewell, Norma. 2003. Dean, College of Life Sciences, University of Maryland. College Park, MD: Interviewed by William Lucyshyn and Jonathan Roberts.
10. Ashcroft, John. 2001. "Memorandum for Heads of All Federal Departments and Agencies." http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm.
11. Beeman, Perry. 1 December 2002. Ag scientists feel the heat. *Des Moines Register*.
12. Bilski, Andrew. 1995. Tokyo Terror. *Maclean's* 108, no. 14.
13. Blanton, Thomas et. al. 2003. "The Ashcroft Memo: 'Drastic' Change or 'More Thunder Than Lightning'?" *The National Security Archive Freedom of Information Act Audit*, Washington, D.C., http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB84/press.htm.
14. Blumenfeld, Laura. 8 July 2003. Dissertation Could Be Security Threat: Student's Maps Illustrate Concerns about Public Information . *The Washington Post*.
15. Bolton, John R., Under Secretary of State for Arms Control and International Security. 2002. Beyond the Axis of Evil: Additional Threats from Weapons of Mass Destruction. Geneva, Switzerland. Fifth Review Conference of the Biological Weapons Convention.
16. Boucher, Richard, Spokesman, Department of State. 2002. Visa Security Reviews.
17. Brickley, Peg. 2003. Science Police Needed? *The Scientist* .
18. Broad, William. 17 February 2002. U.S. Tightening Rules on Keeping Scientific Secrets. *The New York Times*.
19. Brown, DeNeed L. 11 November 2003. A Scholar Confronts 'Ugly Face of America.' *The Washington Post,* p. A17.
20. Card Jr., Andrew H. 2002. "Memorandum for the Heads of Executive Departments and Agencies."
21. Cello, Jeronimo et al. 2002. Chemical Synthesis of Poliovirus cDNA: Generation of Infectious Virus in the Absence of Natural Template. *Science* 297, no. 5583: 1016.

22. Committee on Research Standards and Practices to Prevent the Destructive Application of Biotechnology, Development Security and Cooperation National Research Council. 2003. *Biotechnology Research in an Age of Terrorism: Confronting the Dual Use Dilemma*, The National Academies Press, Washington, D.C.
23. Connolly, Ceci. 28 August 2003. Science Groups Protest Researcher's Treatment. *The Washington Post.*
24. Department of Defense. 1997. *Information Security Program*, DoD 5200.1-R. Department of Defense.
25. Department of Homeland Security. 2004. "Procedures for Handling Critical Infrastructure Information; Interim Rule." *6 CFR Part 29.*
26. Department of Justice. 1981a. Attorney General's Memo on FOIA. *FOIA Update* 2, no. 3.
27. ———. 1981b. Justice Sets New FOIA Policy. *FOIA Update* 2, no. 3.
28. Department of Justice. 2002a. "Freedom of Information Act Guide." Web page, [accessed November 2003a]. Available at http://www.usdoj.gov/oip/foiact.htm.
29. Department of Justice, Office of Information and Privacy. 2002b. "Overview of the Privacy Act of 1974." Web page. Available at http://www.usdoj.gov/04foia/04_7_1.html.
30. Department of Justice. 2003. "Description of Department of Justice Efforts to Encourage Agency Compliance with the Act." Web page. Available at http://www.usdoj.gov/04foia/02rep.htm.
31. Department of State. 2000. "Exhibit 1." *Technology Alert List*, 9 Foreign Affairs Manual 40.31. http://foia.state.gov/masterdocs/09fam/0940031X1.pdf.
32. ———. 2002. "Washington Agency Name Checks." 9 Foreign Affairs Manual 400, http://foia.state.gov/masterdocs/09FAM/09G0400.pdf.
33. ———. 2002. *Using the Technology Alert List: Update.* http://travel.state.gov/state147566.html.
34. Department of Transportation. 2002. Civil Aviation Security Rules. Federal Register.
35. Diabetes Education and Research Center. 1999. "Frequently Asked Questions about Diabetes: What can happen if someone takes too much insulin?" Web page, [accessed 2 April 2004]. Available at http://www.diabeteseducationandresearchcenter.org/info/que3.html.
36. Dobbs, Michael. 3 November 2003. Foreign Enrollment Levels Off at U.S. Schools. *The Washington Post.*
37. Federal Energy Regulatory Commission. 2004. Critical Energy Infrastructure Information – Notice Soliciting Public Comment. Docket Nos. RM02-4-002, PL02-1-002, RM03-6-001.
38. Food Safety Department. 2002. *Terrorist Threats to Food: Guidance for Establishing and Strengthening Prevention and Response Systems.* World Health Organization, Switzerland.
39. Gansler, Jacques S. 2002. Protecting Cyberspace. *Transforming America's Military.* Hans Binnendijk, Washington, D.C: National Defense University Press.
40. Gordon, Lawrence A.; Loeb, Martin P.; Lucyshyn, William. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting & Public Policy*, 461. Elsevier Science Publishing Company, Inc.

41. Gordon-Murnane, Laura. 2002. Access to Government Information in a Post 9/11 World. *Searcher* 10, no. 6.
42. Gugliotta, Guy. 4 October 2001. Agencies Scrub Web Sites of Sensitive Chemical Data. *The Washington Post*.
43. Harmon, Amy. 16 February 2003. Threats and Responses: The Scientists; Journal Editors to Consider U.S. Security in Publishing. *The New York Times*.
44. Hockstader, Lee. 11 November 2003. Post-9/11 Visa Rules Keep Thousands from Coming to U.S. *The Washington Post,* p. A01.
45. Institute of International Education – Open Doors 2003. 2003. *International Student Enrollment Growth Slows in 2002/2003, Large Gains from Leading Countries Offset Numerous Decreases*, press release.
46. Jackson, Ronald J. et al. 2001. Expression of Mouse Interleukin-4 by a Recombinant Ectromelia Virus Suppresses Cytolytic Lymphocyte Responses and Overcomes Genetic Resistance to Mousepox. *Journal of Virology* 75, no. 3.
47. Jacobs, Janice, Deputy Assistant Secretary of State for Visa Services Department of State, and Robert Garrity Jr., Deputy Assistant Director Federal Bureau of Investigations. 2003. The Visa Approval Backlog and its Impact on American Small Business. 108th Cong., 1st sess. House Small Business Committee.
48. Joint Security Commission. 1994. “Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence.” Joint Security Commission, Washington, D.C., http://fas.org/sgp/library/jsc/.
49. Jordan, Mary. 10 November 2003. What Does a Scientist Have to Do With Terrorism? *The Washington Post*.
50. Kay, David. Interim Progress Report on the Activities of the Iraq Survey Group (ISG). House Permanent Select Committee on Intelligence, the House Committee on Appropriations, Subcommittee on Defense, and the Senate Select Committee on Intelligence.
51. Kimberly, Laura L. S. et al. 2002. “Memorandum for Departments and Agencies.”
52. Knezo, Genevieve J. 2002. *Possible Impacts of Major Counter Terrorism Security Actions on Research, Development, and Higher Education*, RL31354. CRS Report.
53. ———. 2003. *Sensitive but Unclassified: and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy*, RL31845. CRS Report.
54. Kumagai, Jean. 2003. Will U.S. Sanctions Have Chilling Effect on Scholarly Publishing? *IEEE Spectrum* Vol. 40, no. 11: 12-15.
55. Leonard, J. William. 2003. *Report to the President, 2002.* Information Security Oversight Office.
56. Metcalfe, Daniel J. 2003. Director (Policy and Litigation), Office of Information and Privacy, Department of Justice. College Park, MD: Telephone interview by William Lucyshyn.
57. Milbank, Dana. 18 December 2003. White House Web Scrubbing. *The Washington Post*.
58. Mintz, John. 12 November 2003. U.S. Fails to Certify Many Labs That Use Pathogens. *The Washington Post,* A13.
59. Mintz, John. 19 February 2004. U.S. to Keep Key Data on Infrastructure Secret. *The Washington Post,* A21.

60. National Science Board. 2002. *Science and Engineering Indicators – 2002*, NSB-02-1. National Science Foundation, Arlington, VA.
61. Neuschatz, Michael and Patrick J. Mulvey. 2003. *Physics Students from Abroad in the Post-9/11 Era*, AIP Pub. Number R-437. American Institute of Physics, College Park, MD.
62. Neustadt, Richard E. 1991. *Presidential Power and Modern Presidents: The Politics of Leadership from Roosevelt to Reagan*. New York: Free Press.
63. Nuclear Regulatory Commission. 1 November 2002. Nuclear Security—Before and After September 11.
64. Office of Security Affairs and Office of Safeguards and Security. 1995. Safeguards and Security Glossary of Terms. Department of Energy.
65. OMB Watch. 2002. "Access to Government Information Post September 11th." Web page, [accessed 6 February 2004]. Available at http://www.ombwatch.org/article/articleview/213/104/.
66. Ornstein, Charles et al. 3 October 2001. Response to Terror. *Los Angeles Times*.
67. Poste, George. 2003. Director, Arizona Biodesign Institute, Arizona State University. College Park, MD: Telephone Interview by William Lucyshyn and Jonathan Roberts.
68. Poulsen, Kevin. 17 December 2003. Secret Service airbrushes photos. *SecurityFocus*.
69. President. 2003a. "Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."
70. ———. 2003b. "Homeland Security Information Sharing, Executive Order 13311."
71. Relyea, Harold C. 2003. Government secrecy: policy depths and dimensions. *Government Information Quarterly* 20, no. 4: 395-418.
72. Reno, Janet. 1993. "Memorandum for Heads of Departments and Agencies." http://www.fas.org/sgp/clinton/reno.html.
73. Rice, Condoleeza. 2001. "Letter to Dr. Harold Brown, Center for Strategic and International Studies." Web page, [accessed November 2003]. Available at http://www.aau.edu/research/Rice11.1.01.html.
74. Schwartz, Stephen I., ed. 1998. *Atomic Audit: The Costs and Consequences of U.S. Nuclear Weapons since 1940*. Washington, D.C.: Brookings Institution Press.
75. Senate. 1997. "Report of the Commission on Protecting and Reducing Government Secrecy." 103d Cong., S. Doc. 105-2, http://www.fas.org/sgp/library/moynihan/chap2.html.
76. Shattuck, Roger. 1997. *Forbidden Knowledge: From Prometheus to Pornography.* 1st Harvest ed. A Harvest Book. San Diego: Harcourt Brace.
77. Shlykhter, Alexander and Richard Wilson. 1992. Chernobyl and Glasnost: The Effects of Secrecy on Health and Safety. *Environment* 34, no. 5.
78. Sinsheimer, Robert L. 1980. The Presumptions of Science. *Economics, Ecology, Ethics Essays Toward a Steady-State Economy.* Herman E. Daly, San Francisco, CA. W. H. Freeman.
79. Sollenberger, Mitchel A. 2004. *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, RS21727. CRS Report.
80. Steinbruner, John et al. 2003. *Controlling Dangerous Pathogens: A Prototype Protective Oversight System*. CISSM Working Papers.
81. Strickland, Lee S. 2003. Visiting Professor, University of Maryland and former

Senior Intelligence Officer, CIA. College Park, MD: Interviewed by William Lucyshyn and Jonathan Roberts.

82. The National Academies. 2002. *Background Paper on Science and Security in an Age of Terrorism*, news release.

83. Union of Concerned Scientists. 2002. *Scientific Integrity in Policymaking: An investigation into the Bush Administration's Misuse of Science*. Union of Concerned Scientists, Cambridge, MA.

84. United States Embassy in Seoul, Republic of Korea. 2003. "Student Visas: Introduction (F 1)." Web page. Available at http://usembassy.state.gov/seoul/wwwh1300.html#sevis.

85. Vest, Charles. 2002. "Response and Responsibility: Balancing Security and Openness in Research and Education." *Report of the President for the Academic Year 2001–2002*, Massachusetts Institute of Technology. http://web.mit.edu/president/communications/rpt01-02.pdf.

86. Weise, Elizabeth. 13 November 2003. Scientists create a virus that reproduces. *USA Today*.

87. Weiss, Rick. 1 November 2003. Engineered Virus Related to Smallpox Evades Vaccine. *The Washington Post*.

88. Withnell, Elizabeth. 18 February 2004. Letter to Steven Aftergood.

About the Authors

The Honorable Jacques S. Gansler, former Under Secretary of Defense for Acquisition, Technology, and Logistics, is the University of Maryland's Vice President for Research and the Roger C. Lipitz Chair in Public Policy and Private Enterprise. As the third-ranking civilian at the Pentagon from 1997 to 2001, Professor Gansler was responsible for all research and development, acquisition reform, logistics, advance technology, environmental security, defense industry, and numerous other security programs. Before joining the Clinton Administration, Dr. Gansler held a variety of positions in government and the private sector, including Deputy Assistant Secretary of Defense (Material Acquisition), assistant director of defense research and engineering (electronics), executive vice president at TASC, vice president of ITT, and engineering and management positions with Singer and Raytheon Corporations. Throughout his career, Dr. Gansler has written, published, and taught on subjects related to his work. He is a member of the National Academy of Engineering and a Fellow of the National Academy of Public Administration. Additionally, he is the Glenn L. Martin Institute Fellow of Engineering at the A. James Clarke School of Engineering, an Affiliate Faculty member at the Robert H. Smith School of Business and a Senior Fellow at the James MacGregor Burns Academy of Leadership (both at the University of Maryland). For 2003–2004, he served as Interim Dean of the School of Public Policy.

William Lucyshyn is a Research Director at the Defense Advanced Research Projects Agency (DARPA) and a Visiting Senior Research Scholar at the Center for Public Policy and Private Enterprise in the School of Public Policy at the University of Maryland. In this position, he conducts research into the public policy challenges posed by the increasing role information technologies play in improving government operations and their relationships with the private sector. Previously, Mr. Lucyshyn served as a program manager and the principal technical advisor to the Director, DARPA, on the identification, selection, research, development, and prototype production of advanced technology projects. Prior to this appointment, Mr. Lucyshyn completed a 25-year career in the U.S. Air Force serving in various operations, staff, and acquisition positions. Mr. Lucyshyn received his Bachelor Degree in Engineering Science from the City University of New York in 1971. In 1985 he earned his Masters Degree in Nuclear Engineering from the Air Force Institute of Technology. He was certified Level III as an Acquisition Professional in Program Management in 1994.

Graduate Research Assistant

Jonathan A. Roberts is now a law student at American University, Washington College of Law. In 2004, he earned a Masters Degree in Public Policy, concentrating in International Security and Economic Policy, also from the University of Maryland, where he was a research assistant for the Center for Public Policy and Private Enterprise. In addition to researching information security policy, he also assisted in the preparation of case studies related to competitive sourcing. Mr. Roberts previously served as a research assistant in the Department of Cell Biology and Molecular Genetics, investigating pre-mRNA splicing factors and oligonucleotide bias in *Drosophila melanogaster*. He has also conducted research with the Computer Science Department, introducing tools for detecting faults in Internet Protocol networks and cross-disciplinary techniques for analyzing the politico-economic drivers of regional integration. He received Bachelors Degrees in Computer Science and Government and Politics (with honors) from the University of Maryland in 2003.

UNIVERSITY OF
18 56
MARYLAND

CENTER FOR PUBLIC POLICY AND PRIVATE ENTERPRISE
SCHOOL OF PUBLIC POLICY

Strengthening Connections to Improve Policy and Management

The Center focuses on areas impacted by public-private networks; including, government sourcing, supply chain management, national security, information assurance, and economic competitiveness.

www.cpppe.umd.edu