Global Information Assurance Certification Paper

Alexander J. Breeding
SANS Security Essentials GSEC Practical Assignment
Version 1.4b – Option 1
August 22, 2003

Sensitive but Unclassified Information:

A Threat to Physical Security

Table of Contents

INTRODUCTION

Considerable effort has gone into analyzing the possibilities of an "electronic Pearl Harbor" attack against the United States. While theories about the possibilities of cyber warfare and terrorist attacks on United States soil have been debated since the mid-1990s, life for all Americans changed on September 11, 2001. We have an enemy or enemies who have demonstrated their willingness to attack us with unconventional means on our home soil. While we have expended great efforts into defending our company networks against hackers, viruses and worms, let us not overlook the fact that the biggest threat to our critical infrastructures, and even our buildings, does not lie in cyberspace. Far more damage can be affected in the physical world. We must consider this new reality when we post information on to a website. We must consider the real possibilities of publicly available information becoming a threat to physical security.

Defending our companies and the "critical infrastructure" of the United States must be extended to include physical security. Defending the physical security of a company or other critical assets does not lie in the exclusive domain of the security guard. That duty extends also to the information department. We must be diligent in protecting information that could lead to disastrous attacks on our own companies and/or the critical infrastructure of the United States, to include "sensitive but unclassified" information. This information must be removed from any current website, and must also be cleansed from cached web pages maintained for reference purposes.

VULNERABILITIES

Vulnerabilities have been defined most simply as weaknesses. In the information realm, we generally only consider those vulnerabilities that apply to our various computer systems. After all, that is our training and our occupation. We want to protect our systems from various weaknesses, and with good reason. The vulnerabilities that can exist in cyberspace can be extremely dangerous. The following is from the National Strategy to Secure Cyberspace:

> By exploiting vulnerabilities in our cyber systems, an organized cyber attack may endanger the security of our Nation's critical infrastructures. Cyberspace vulnerabilities occur in the critical infrastructure enterprises and government departments themselves, in their external supporting structures (such as the mechanisms of the Internet), and in unsecured sites across the interconnected network of networks. Vulnerabilities exist for several reasons including technological weaknesses, poor security-control implementation, and absences of effective oversight.[1]

Specifically articulating the wide range of vulnerabilities that are currently known for computer systems is beyond the scope of this paper. It is sufficient to state

the obvious fact that there are many known vulnerabilities and new ones being discovered every day. However, perhaps the most glaring vulnerabilities do not exist in our computer systems, but because of our computer systems.

Prior to the September 11 attacks, few people considered the possibility that providing detailed information regarding various control systems or building layouts could be endangering their physical safety. Today we know better, although there is still a wealth of information available online. According to former computer crime director for the Department of Justice, Eric Friedberg,

> Many web sites constitute a gold mine for potential attackers. Audits have found descriptions of physical locations of backup facilities, the number of people working at specific facilities, detailed information about wired and wireless networks, and specifications of ventilation, air conditioning and elevator systems. Other sites give graphical representations of floor plans, cabling connections, and ventilation ductwork. [2]

Some seem unconcerned. "Our floor plan is not a whole schematic of the building", stated Mike Howard, leasing manager for American Executive Centers. American Executive Centers offers photographs, floor plans and virtual tours of their buildings online.[3] This kind of apathy is in direct conflict with the National Infrastructure Protection Center's (NIPC) requests to all companies and government agencies "to scour their public websites for sensitive information pertaining to critical infrastructure systems." [4]

In spite of the requests by the NIPC, sensitive information remains freely available on the Internet, some of which could have disastrous consequences. In recent days, investing very little time, I've been able to discover the exact location of every nuclear reactor in the United States and other countries. [5] Not only have I found the exact location of these reactors, I have also pinpointed their locations on maps using GPS, and even just plain old web pages. I have additionally been able to obtain pictures of the reactors from terraserver. [6] This has made it very easy for me to know exactly what my target would look like if I desired to fly an airplane into one. Additionally, I have found a map of the routes of travel from various states, via highway and rail, to the Nevada nuclear waste facility in Yucca Mountain. [7] It is extremely unwise for this information to be published at all, especially on a world wide, freely accessible medium.

THREATS

There are numerous threats to the nation's critical infrastructure today, both cyber threats and physical threats. Most notably, terrorists and hostile nation-states pose a realistic danger, and this danger is more likely to be to physical assets rather than cyber assets.

"Physical destruction is still the greatest threat" to our Nation's critical infrastructure. [8] In spite of this statement having been made in 1997, some 6 years ago, recent terrorist activity plainly indicates that this is still true.

Still other threats exist to cyber systems. There has been a continuing increase in questionable cyber activity over the years. Script kiddies and virus writers make up only part of this group. Surely industrial espionage and true cyber reconnaissance are taking place, in addition to genuine hacking issues.

In August of 2003, it was reported that the "Slammer Worm" penetrated a network at the Ohio Davis-Besse nuclear power plant. This worm disabled a safety monitoring system for nearly 5 hours [9]. Allegedly, this breach did not cause a safety hazard. But the thought of the protection systems on a nuclear reactor being disabled for any amount of time is troublesome. Let it never be said that worms and viruses pose no real threat.

Given the potential for large-scale disasters, cyber threats can be especially troublesome, especially concerning the sophistication of some terrorist networks. Should they ever coordinate a physical attack with a cyber attack, the consequences could be dire, indeed.

These, of course, are not the only types of threats to our systems. There are other obvious threats to consider when planning for physical interruptions to business – fire, flood, tornado, etc. These types of things are normally considered in a disaster recovery/business continuity plan. However, I would offer that the physical destruction of a building is rarely considered as a viable threat of information warfare. I dare say that in light of the evidence above, publicly available information could result in physical destruction. We must consider physical security and the protection of our physical assets as an integral part of a security plan. Terrorism, in many forms, is currently our biggest threat.

TERRORISM

What is terrorism? Terrorism has been defined as "The unlawful use of – or threatened use of - force or violence against persons or property to coerce or intimidate governments or societies." [10] Obviously, one who commits acts of terrorism is a terrorist. There are both International terrorist groups (organizations or individuals located primarily outside of the United States whose operations can be conducted in any territory [al Qaeda]), and Domestic terrorist groups (organizations or individuals located and operating entirely within the United States or its possessions whose operations are directed at the United States [Timothy McVeigh]).

Additionally, there are different types of terrorist organizations. Some terrorist groups are state-sponsored, which is to say that they receive support from the government of certain states. These groups generally operate independently but

do receive funding from certain states. They will usually attempt to operate in the best interests of their sponsoring states, but not always.

There are also state-directed terrorist groups. These groups are generally acting on behalf of a government. They receive not only funding, but also receive direction from the state, and operate with the full knowledge of the government. There are also non-state sponsored terrorist groups. These groups operate independently of any government and receive no substantial support from any government.

Terrorist Objectives

Terrorist attacks are generally classified according to the immediate terrorist objectives. Common objectives can include recognition, coercion, intimidation, provocation and insurgency support. [11]

Recognition

The objective of some types of terrorist attacks is for the sole purpose of recognition for the organization. Recognition can develop support and funding from various sources, and also aids in recruiting new members. These types of attacks are often meant to demonstrate the strength of an organization or prove their ability to attack anyone anywhere.

Coercion

Coercion is an attempt to make an individual or government act in such a way as the terrorist group dictates. These types of attacks are usually directed at selective targets and intended to induce massive destruction.

Intimidation

Although this type of attack is very similar to coercion, its primary motivation is to prevent an individual or government from action rather than force said action. This type of attack is common in the Israeli/"Palestinian" conflict, wherein the suicide bombers supporting the "Palestinians" will kill a group of innocent Israelis in an attempt to intimidate the Israeli forces or Government from jailing other suspected terrorists.

Provocation

This type of attack is intended to provoke a massive retaliatory strike from the victim. These types of attack are normally launched against a symbol of a government's authority and are designed to show their government's vulnerability. These attacks are carried out to weaken faith in the government as well as gain publicity and perhaps sympathy for the terrorist's cause.

Insurgency Support

Terrorist groups can support various insurgencies in smaller countries. They will usually benefit greatly from supporting a rebel cause in countries where the government is already unstable. By supporting the rebels, the terrorist organizations tend to develop safe havens should the rebels be successful. If the rebellions fail, the terrorist groups will have made a friend in those who already practice the same tactics. They also can gain as allies those who provide support and comfort to the rebels.

Terrorist Tactics

At a fundamental level, all terrorist activity seeks to create fear and further their cause or objectives. To achieve those goals, traditional terrorist tactics include:

- Assassinations
- Armed assaults and kidnappings
- Murders
- Bombings
- Hijackings

However, never let it be said that terrorists are not forward thinking. Terrorists still utilize the above mentioned methods, however, they have also begun to exploit the following tactics:

- Cyber warfare
- Product contamination
- Affecting the Critical Infrastructure

While conducted by an individual, not an organization, at a fundamental level, the cyanide poisoning of Halloween candy (pixie stix) in Houston in the 1970's and the Tylenol poisoning in the 1980's was a form of product tampering. [12] We've all been warned continuously of the so-called "electronic Pearl Harbor" that's coming. Not only will this type of cyber warfare including the standard hacking, viruses and worms, but it is said to include logic bombs and other forms of code that have been dropped onto machines previously and will go off at a specified time or with additional instructions. Certain types of these attacks have been perpetrated in the past with machines becoming "zombies" in DDoS attacks. Some of these cyber warfare attacks are suspected of being able to affect the critical infrastructure of the country, as well. However, the vast majority of terrorists' targets have been in the past and remain physical targets. "The threat of cyberterrorism is far outweighed by the threat posed to the U.S. homeland by traditional, more violent, forms of terrorism." [13]

RECENT EVENTS

Most of the tactics described above are clearly physical attacks. The most obvious "recent" terrorist attack on the United States is the destruction of the two towers and other buildings at the World Trade Center in New York. In these attacks, terrorists hijacked airplanes and flew them into both towers. The resulting fires ultimately collapsed both of the towers. Thousands were killed. Additional attacks that day caused damage to the Pentagon and additional loss of life in Pennsylvania. These attacks were coordinated, physical attacks, although information was undoubtedly obtained through the Internet. [14] These terrorists used multiple avenues to obtain the information they needed to cause such mayhem. Could these attacks have been thwarted by the removal of certain information from various Internet sites? Unlikely, but we'll never know.

What we do know is that there is a wealth of information available on the Internet. According to Google, there are currently 3,083,324,652 indexed pages online. And while the NIPC has issued multiple statements asking private companies and various government agencies to remove sensitive information, as previously mentioned, there's lots of it remaining online. In addition to the aforementioned nuclear waste transportation routes, I also found a map of every electrical power generating station in California. The map was broken out by county and listed each plant, it's location and the type of power plant it was (biomass, coal, digester gas, nuclear, etc.).[15] On the same site, a state government site by the way, I found a map detailing California's major electric transmission lines.[16] How convenient for terrorists. They don't even have to compile any information to obtain a detailed target listing.

Of course, the Internet is not the only source of information in today's world. There are other ways to learn. It's possible to learn how to fly airplanes by purchasing flight simulation software. It's also possible to learn to fly by watching either public television or other "science channels" via cable or satellite television. It's also possible to learn by reading books. And while I am not advocating any real censorship, I do believe that certain information should be more tightly controlled. Obviously, airlines have to publish their schedules so people can book flights. Would be hijackers will have easy access to this type of information. But how did they know that early morning flights from the East coast to the West coast on Tuesday mornings normally have a small passenger load? This information was undoubtedly available from some organization, and probably was freely available online.

For an even more disturbing picture, consider the following information taken from a recent article in the Washington Post entitled "Dissertation Could Be Security Threat" by Laura Blumenfield.

> … Gorman's work has become so compelling that companies want to seize it, government officials want to suppress it, and al Qaeda operatives – if they could get their hands on it – would find a terrorist treasure map.
>
> Tinkering on a laptop, wearing a rumpled t-shirt and a soul patch goatee, this George Mason University graduate student has mapped every business and industrial sector in the American economy, layering on top the fiber-optic network that connects them.
>
> He can click on a bank in Manhattan and see who has communication lines running into it and where. He can zoom in on Baltimore and find the choke point for trucking warehouses. He can drill into a cable trench between Kansas and Colorado and determine how to create the most havoc with a hedge clipper. Using mathematical formulas, he probes for critical links, trying to answer the question: "If I were Osama bin Laden, where would I want to attack?"

Clearly, if a graduate student at a college in Virginia can find all of this information, so can everyone else. Is this type of information sensitive? According to Richard Clarke, former White House special advisor for cyberspace security to President Bush, "The fiber-optic network is our country's nervous system. You don't want to give terrorists a road map to blow that up." [17]

So assuming the protection of assets and person is important, should this type of information be available online? I am suggesting that certain types of information be more closely held rather than being so freely available. What types of information should this encompass? For starters, information about the "critical infrastructure" of the United States should be included. This information must be considered, at the very least, "sensitive but unclassified."

CRITICAL INFRASTRUCTURE

A very obvious definition of critical infrastructure would be the infrastructure that is crucial to the normal conduct of daily operations. A more complete definition of critical infrastructure is set out in various U.S. Government documents and is summarized below.

> Critical infrastructures are those systems and assets which are so vital to the United Sates that the incapacity of such systems and assets would have a debilitating impact on the country's ability to function, or would have a deleterious effect on the country's morale. [18]

Further, infrastructure has been defined as

> the framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and

distribution capabilities that provide a flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole. [19]

That definition is all well and good, but what specifically is involved in the critical infrastructure? The types of systems that make up the critical infrastructures include:

- electric power generation plants (including nuclear power generators) and distribution systems,
- gas and oil production and distribution systems,
- e-commerce systems and banking (including the stock exchange),
- water treatment facilities and fresh water distribution systems,
- telecommunications (including both voice and data systems, and wireless systems),
- transportation (including roads and airlines),
- agriculture (food, meat and poultry),
- health services and
- police and fire departments.

Chemical plants and hazardous materials (including nuclear waste) should also be considered part of this group, as they can be targets for terrorist attacks due to the fact that chemical plants could be used as sources of materials for terrorists' weapons. The exposure of the surrounding community to large quantities of the chemicals created or stored in the plant also could kill or sicken the community. Additional components of the critical infrastructure could be companies heavily involved in the defense industry, the postal service and other shipping companies. Certainly National Monuments and Icons belong in this group because of the phrase "deleterious effect on the country's morale" being added by the Bush administration to the definition of critical infrastructures. Others also consider the GPS (global position system) frequencies and all Federal computer networks to be part of the critical infrastructure. [20]

These types of systems were first addressed during the Clinton administration, and studied by the President's Commission on Critical Infrastructure Protection (PCCIP). This group was created in July 1996 and was tasked with assessing the vulnerabilities of the country's critical infrastructures and proposing a strategy for protecting them. In response to the recommendations of the Commission, President Clinton created Presidential Decision Directive No. 63 (PPD-63). This Directive instructed the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism and other government officials to consult with private sector owners and operators or critical infrastructures, and encourage the creation of a private sector information analysis and sharing center. [21]

In furtherance of the protection of the critical infrastructure, President Bush proposed the establishment of the Department of Homeland Security. [22] This

proposal included a function whose responsibilities include the coordination of policies and actions to protect the nation's infrastructure. However, this proposal did not specify how to determine criticality or which infrastructure should be considered critical.

Several documents have been proffered over the last few years concerning critical infrastructure protection containing general definitions and lists of infrastructures that should be included. However, none of these lists have been accepted as definitive. As our economy and culture have continued to change, so these lists have expanded over time. Originally, critical infrastructures were considered to be "those whose prolonged disruptions could cause significant military and economic dislocation." [23] Now included in these lists are national monuments (the Vietnam Veteran's Memorial Wall) where terrorist attacks could cause large loss of life or have a deleterious effect on the nation's morale.

There is some debate ongoing in various government agencies as to the true critical nature of every infrastructure category currently on the list. [24] Additional studies would be required to identify those elements most critical. These studies should be completed immediately. It is vitally important that we appropriately identify the most critical elements and prioritize immediate actions to follow a terrorist event in this country. Much like the continuing life cycle of any security, business continuity and disaster recovery plan,[25] the critical nature of the infrastructure should be constantly evaluated and updated. Additionally, appropriate government agencies should concentrate on areas of overlap in the various infrastructures. So-called cross-roads, intersections or interdependencies should be identified and any vulnerabilities taken into account. Also high priority should be given to geographic areas where a large number of infrastructures exist, such as the Los Angeles area where there are a number of electrical power plants and distribution systems, large numbers of oil refineries, chemical plants, transportation hubs and shipping ports.

In PPD-63, critical infrastructures were defined as "those physical and cyber-based systems essential to the minimum operations of the economy and government." [26] However, this Directive did not articulate the distinction between physical security and cyber security, making the appropriate response for the businesses involved somewhat confused.

For example, the physical assets of an electrical power plant normally include the generating plant itself, the turbines and other equipment inside, and distribution lines and towers. The computer hardware and communication lines that help control the flow of electricity, however, could be considered either a physical asset or a cyber asset. The data transmitted and stored on the computers and the software that controls the processes are normally considered cyber assets. Physical security is generally concerned with protecting the physical assets, including computers, from damage caused by physical forces (such as explosion, theft, weather damage, etc.). Cyber-security generally means protecting the

software, data and processes operating on the computer systems. With the emergence of telecommuting and more automated systems, however, cyber security now is concerned with preventing access to those systems remotely and can even be considered to be protecting power distribution (or at least the power distribution system). Physical and cyber protection obviously have some overlapping areas of responsibility, in spite of their seemingly disparate nature. Clearly better cooperation and understanding between those responsible for physical security and those responsible for cyber security is needed.

As early as 1995, the National Intelligence Council was studying potential attacks on the public switched telephone network and Supervisory Control and Data Acquisition (SCADA) systems – the computers that control electrical power distribution, oil refineries, and other similar utilities. [27] The following year, John M. Deutch, then Director of Central Intelligence said "Protecting our critical information systems and information-based infrastructures is a subject that is worthy of considerable attention and is an issue that I am deeply concerned about." [28] Later in that same speech, Deutch stated "we should not forget that key nodes and facilities that house critical systems and handle the flow of digital data can also be attacked with conventional, high-explosives." Of greatest concern was that hackers, terrorist groups or other countries might seriously disrupt "infrastructures such as electric power distribution, air traffic control, or financial sectors." [29]

And while it was not an attack specifically aimed at the critical infrastructure, the World Trade Center attack in September 2001 certainly disrupted portions of the critical infrastructure. The attacks "immobilized the nation's air traffic and disrupted telecommunications and transportation infrastructure, emergency services and government operations." [30]

Following the attacks, Con Edison's energy infrastructure in lower Manhattan was significantly impacted. At the time, Con Edison was the sole provider of electrical power to lower Manhattan. The collapse of 7 World Trade Center permanently damaged two substations located near the building and also damaged major electric transmission cables. A third substation near the South Street Seaport also lost service resulting in over 12,000 customers being without electricity. Electric power was also lost over significant portions of lower Manhattan. In order to attempt speedy resolution, Con Edison placed temporary facilities in service and isolated the WTC area from the system as best they could. Certain areas were still unsafe following the collapse of several buildings at the WTC site. Con Edison dispatched over 140 crews (over 300 people) to work in the WTC vicinity to inspect and test equipment, prepare work locations and coordinate effort with emergency agencies. [31]

Following the September 11 terrorist attacks, President Bush signed new Executive Orders relating to critical infrastructure protection. [32] E.O. 13228, signed October 8, 2001, established the Office of Homeland Security and the

Homeland Security Council. This office was to "coordinate efforts to protect critical infrastructures ...[and]… work with federal, state, and local agencies and private entities to:

> Strengthen measures for protecting energy production, transmission, and distribution services and critical facilities; other utilities; telecommunications; facilities that produce, use, store, or dispose of nuclear material…;
>
> …coordinate efforts to protect critical public and privately owned information systems…;
>
> …to ensure that special events determined by appropriate senior officials to have national significance are protected…;
>
> …to protect transportation systems within the United States, including railways, highways, shipping ports and waterways, and airports and civilian aircraft…;
>
> …to protect United States livestock, agriculture, and systems for the provision of water and food for human use and consumption… [33]

President Bush also signed Executive Order 13231, creating the President's Critical Infrastructure Protection Board. [34] In spite of the obvious need for true critical infrastructure protection, this Board oversees primarily information infrastructure. They do, however, recognize the importance of "telecommunications, energy, financial services, manufacturing, water, transportation, health care and emergency services." [35]

Critical infrastructures were further defined under the USA PATRIOT Act (P.L. 107-56), passed in October of 2001. Section 1016 of the Act defined critical infrastructures as:

> …systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health and safety, or any combination of those matters. [36]

Other sections of the Act further defined the types of critical infrastructures intended to be covered by the Act. A companion document, the draft legislation proposing the Office of Homeland Security, stated the Department would build and maintain a comprehensive assessment of the nation's following infrastructure sectors:

- Food
- Water

- Agriculture
- Health systems and emergency services
- Energy (electrical, nuclear, gas and oil, dams)
- Transportation (air, road, rail, port, waterways)
- Information and telecommunications
- Banking and finance
- Chemical
- Defense industry
- Postal and shipping
- National monuments and icons

A further delineation of critical infrastructure as compared to key assets was set forth in *National Strategy for Homeland Security*, a document released by the Bush Administration in July of 2002. Key assets were defined as individual targets whose "destruction would not endanger vital systems, but could create local disaster or profoundly damage our nation's morale and confidence." [37] These key assets included historical attractions and local facilities, such as schools and courthouses. The reason for including some local assets could have been to offer Federal monetary resources to assist in protecting them.

Of course, the more recent "Blackout of 2003" paints an even more disturbing picture. Somewhere in Ohio, three high capacity transmission lines failed and shut down. For some as of yet unknown reason, the "grid" did not react as anticipated. Rather than isolating that area of the state, all interconnections continued. The entire "northeastern" third of the United States and parts of Canada were open to failure because of this. [38] This entire area did, in fact, experience a prolonged outage of power. This was not caused by a terrorist act, allegedly, although none can say conclusively what did cause this outage. Clearly, the electrical power generation and distribution systems of the United States are a major part of the critical infrastructure. Clearly, these systems are vulnerable. Imagine what would happen if terrorist coordinated an attack on all major interconnected grids across the United States, in a similar fashion as the attacks on the World Trade Center in 2001. How much work could get done without electricity? Consider the food and beverage industry, for instance, the local grocery store. Many beverages spoil quickly without refrigeration, as do many food products. Refrigeration requires electricity in most parts of the world. Without electricity, the spoilage of very large portions of inventory would have disastrous effects on grocery, food and beverages businesses. This would be only one small outcome of such an attack.

So now that we have this rather cumbersome definition of the critical infrastructure, let's consider the scope of what is actually covered.

WHAT IS THE SCOPE?

A recent report by the National Research Council described the U.S. domestic transportation system as follows:

> The U.S. highway system consists of 4 million interconnected miles of paved roadways, including 45,000 miles of interstate freeway and 600,000 bridges. The freight rail networks extend for more than 300,000 miles and commuter and urban rail systems cover some 10,000 miles. Even the more contained civil aviation system has some 500 commercial-service airports and another 14,000 smaller general aviation airports scattered across the country. These networks also contain many other fixed facilities such as terminals, navigation aides, switch yards, locks, maintenance bases and operation control centers. [39]

Of course, this does not cover any of the inland waterways or other maritime facilities that should be included in the transportation system.

Additionally, the electric power infrastructure includes some 92,000 electric generating units of various types (fossil fuel, nuclear and hydroelectric), 300,000 miles of transmission lines, and 150 control centers regulating the flow of electricity. The water infrastructure of the US includes 75,000 dams and reservoirs, thousands of miles of pipes and aqueducts, 168,000 public drinking facilities, and 16,000 publicly owned waste water treatment facilities. And the chemical industry has thousands of facilities that handle hazardous or toxic substances. [40]

Considering all of this in such a small percentage of those industries covered by "critical infrastructure", how can we possibly protect everything? And the answer, of course, is we cannot. So what to do? Again, we must prioritize our protection scheme. In order to do this, we must analyze available data and gather any necessary data should what we have already prove to be inadequate. This data must be analyzed to reveal what is truly critical in the critical infrastructure, and thereby enumerate our priorities.

For instance, the National Highway System makes up only 4% of the total mileage of the system, but it carries over 44% of the nation's travel. The highway system also carries practically 100% of the nation's food supplies between production and public outlets. Similarly, there are 546 airports that had commercial airline service in April 2001, but 70% of the nation's air travel originated at just 31 airports. [41]

And while there are obviously hundreds of Internet and telephone service providers, the fiber-optic network of the United States is not provided by those

hundreds of companies. The major portions of the fiber-optic network nationwide are provided by only a handful. Yet, these networks carry the Internet, telephone calls, cell phones, military communications, bank transfers, air traffic control signals, rail and highway traffic controls, and water systems and power grid Supervisory Control And Data Acquisition (SCADA) controls.

Part of the concern of physical attacks is the vulnerability of Supervisory Control And Data Acquisition (SCADA) systems. These systems are used to either remotely control certain procedures or to constantly monitor and/or update systems. [42] If a terrorist were aware of these types of systems being utilized by an intended target, the easiest way to negate abilities of these systems would be to simply cut the phone lines or blow up the nearest phone switch. Either of these actions could render these SCADA systems useless. Even the SCADA systems themselves sometimes adversely affect the critical infrastructure. [43] The easiest way to determine the types of equipment are being used is to check the company's website. [44] This is especially true in the case of electrical power companies. They tend to try to lure customers with their advanced technology. These companies tout it on their television commercials, and on their (arguably) most effective communication tool, their website.

The Internet has changed the way companies conduct business. Prior to 2000, few companies did much business via e-commerce on the web. Most, if not all, previous electronic transactions were conducted on private exchanges or VANs. Little if any business was conducted on the Internet. Now many companies exist solely as web-based entities. All of their business is conducted online, including their monetary transactions. Additionally, many companies conduct remote access to provide their employees e-mail and access to network resources. And some companies handle numerous procedures to conduct their business via remote access. This is why there is such a concern over cyber warfare.

Of course, what's not taken into account when considering cyber warfare is the amount of data that's published online. There are literally billions of web pages in existence today. There are also lots of pages that have been gathered, indexed and cached even though they are no longer online in their original location. This makes this information still available to anyone, including those who would use it nefariously. This is the real battleground for information warfare. The Internet is the storage house of information for terrorists. The protection of this information must be ensured.

CLASSIFICATION

While this information should be protected, I am not advocating censorship. Yet, the protection of this sensitive information must be assured. Earlier I mentioned Sean Gorman, the graduate student at George Mason University who has compiled a "vulnerability super map". According to the story in the Washington Post, he "compiled his mega-map using publicly available material he found on

the Internet. None of it was classified." [45] Should this type of information be classified? What, exactly, do we mean by classified?

There are various Government and military organizations possessing the authority to classify materials. Classified materials normally fall into three categories: confidential, secret and top secret. [46] Various organizations throughout the United States have the ability and responsibility to classify sensitive material. One such organization is the Department of Energy. They have an Office of Safeguards and Security Evaluations to assist the Secretary of Energy in securing sensitive information. Other organizations have similar oversight groups, although by directive there are only 29 individuals specifically accountable for classifying documents. [47] They are also empowered to appoint others to assist them, and this is where most information is classified. By directive, these individuals are also responsible for the "trickle down" bits of information, such as those Sean Gorman used to compile his map. These bits of information are harmless on their own, yet when compiled, they can reveal astonishing amounts of sensitive information.

In order to protect information, the Government has issued NSDD-189 in 1985 [48] and Executive Order 12958 in 1995 [49] that describe the general classification policy. In section 1.5 of Executive Order 12958, it states that scientific, technological, or economic matters relating to the national security may be classified. It further states in section 1.8b that basic scientific research information not clearly related to the national security may not be classified.

Following the September 11, terrorist attacks, the Bush administration sought to gain tighter control of information publicly available. In a memo from President Bush's Chief of Staff Andrew Card to executive branch departments and agencies, a copy of which can be viewed at http://www.fas.org/sgp.bush/wh031902.html, in March of 2002, Card warned that information held by government agencies that could reasonably be expected to provide direction or assistance in the construction or use of weapons of mass destruction should not be disclosed. [50] He additionally suggested tighter control of "sensitive but unclassified" information.

Sensitive but unclassified has not been fully defined, but was "hinted at" in the memo as follows:

> The need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information. [51]

Here, a conflict appears between protection and free exchange of information. Again, we consider a government agency's guidelines of sensitive but unclassified. The following is from the State Department:

> … information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. [52]

As previously mentioned, the Department of Energy also controls documents of a sensitive nature. Here's how they describe sensitive but unclassified:

> Information for which disclosure, misuse, alteration or destruction could adversely affect national security or government interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the Federal Government. Governmental interests are those related, but not limited to, the wide range of government or government-derived economic, human, financial, industrial, agricultural, technological, and law enforcement information, as well as the privacy or confidentiality of personal information provided to the Federal Government by its citizens. [53]

The Defense Department maintains several types of controlled but unclassified information. According to information obtained from their website (http://www.dss.mil/search-dir/training/csg/security/S2unclas/Intro.htm), they have defined sensitive but unclassified information as "For Official Use Only. They further define Official Use information as: "a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the Freedom of Information Act." [54]

With all of these differing definitions, how are we supposed to know what is sensitive information? Sensitive has been defined again as

> information related to systems, structures, individuals and services essential to the security, government or economy of the State, including telecommunications … electrical power, gas and oil storage and transportation, banking and finance, transportation, water supply, emergency services … and the continuity of government operations. [55]

This sensitive but unclassified designation has angered at least three "prestigious" government science academies. [56] They have urged the Bush administration not to classify documents with this label. Allegedly, thousands of documents have been removed from Government websites and libraries. [57] The National Academy of Sciences, the National Academy of Engineering and the Institute of Medicine have said the withholding of this information "could stifle scientific creativity" and actually weaken national security. This, of course, is the same argument hackers use when exposing hacks to the public rather than to the vendor or scientific community first. They claim that only by exposing the weaknesses to the general public will the vendor fix the problem. Of course,

exposing the weakness leads to the weakness being exploited. A prime example of this is the recent Blaster worm that was designed to create a DDoS attack against the Microsoft Update webpage. [58]

Federal Controls on Privately Generated Scientific and Technical Information

The Government has put procedures into place over the years to allow for access to sensitive information by means of the Freedom of Information Act (FOIA). [59]

There are additional concerns over the protection and classification of information because of the rights guaranteed to an individual under the First Amendment of the Constitution. It states: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." But do individuals really have a right to say anything they want? No. And do individuals really have a right to obtain any information they want? No. So again the conundrum appears. How do we provide the appropriate protection to the United States and the critical infrastructure we all depend on while at the same time provide for free and open access to information? There must be a way to balance these opposing sides.

There are several laws currently in place that allow the federal government to classify, and therefore, control access to privately-generated scientific and technical information – provided free access to this information could harm national security. The majority of these laws deal with patent law secrecy and atomic energy data.

Patent Law Secrecy

The U.S. Patent Commissioner has the right to issue patent secrecy orders to prevent information being disclosed about an invention that might prove harmful to the national security of the United States. [60] This ability to prevent the release of such information is true regardless of whether the United States has a "property interest" or not. If the government does hold a property interest, the Patent Commissioner is notified by the appropriate agency head and no information is published regarding the application or the granting of a patent. In the case of privately-held information wherein the government does not hold a property interest, should the Patent Commissioner decide the publication of the information in question could harm the national security, he must present the patent application to the head of the relevant government agency. Should it be determined that the publication of such information is detrimental to the national security, the Patent Commissioner will order the invention be kept secret, and "shall withhold the grant of a patent … for such period as the national interest

requires …". The inventor may appeal to the Secretary of Commerce if an invention is deemed secret. The invention may be kept secret for a period of one year, but the Secretary of Commerce may renew the secrecy order for additional periods upon recommendation by the initial agency head who determined the need for secrecy. [61]

The Atomic Energy Act and "Restricted Data"

The original concept of "need to know" was developed during the atomic energy research conducted at the beginning of World War II. The scientists working on the Manhattan Project endeavored to keep their work secret from all, except those with a need to know. Following the war, Congress passed the Atomic Energy Act of 1946 (60 Stat. 755). This established the Atomic Energy Commission (now the Department of Energy) and rules for maintaining the secrecy of atomic energy information. These laws allow the government to limit access to "all atomic energy-related information, which is automatically 'born classified' and is categorized upon creation as 'restricted data'." [62] These laws were amended by the Atomic Energy Act of 1954 which allowed for some access to restricted data for the purposes of "peaceful commercial development of atomic energy." [63]

Currently, restricted data is defined as "all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted data category pursuant to section 142". [64]

Export Control

Of course, there are also restrictions on exporting technologies, information or weapons that could provide assistance to foreign individuals or governments in any potential attempts to take hostile action against the United States. These restrictions include the Export Administration Act [EAR](50 U.S.C. App. 2401-2420) [now expired but effectually operating under the International Emergency Economic Powers Act (IEEPA) pursuant to Executive Order 13222 of August 17, 2001] and the Arms Control Act (22 U.S.C. 2751-2794). As you are probably aware after opening any package of commercial off-the-shelf technical software package, there are laws regulating the export of technical data. Technical data is defined under the Export Administration Regulations (15 CFR 772.1) as "Information of any kind that can be used, or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials." [65] This is not to suggest that technical data may not be exported at all. But in order to export technical data, including publishing such data on the Internet, you must have a license issued by the Department of Commerce or State Department.

Herein lies another confusing issue. While the regulations followed by the State Department (International Traffic in Arms Regulations [22 CFR 120.10]) treat the disclosure or transfer of technical data to a foreign national as an export, again including publication of such data on the Internet, they do not consider "publicly available scientific and technical information and academic exchanges and information presented at scientific meetings" as controlled technical data. Specifically omitted from this definition is information in the "'public domain', if published and generally available and accessible to the public through, for example, sales at newsstands and bookstores, subscriptions, second class mail, and libraries open to the public". [66] This is especially troubling considering the label sensitive but unclassified.

However, under the EAR regulations, the Commerce Department considers exports to foreign nationals of sensitive technical data or those countries defined as "sensitive" according to 15 CFR 734.2(b). Again, these are considered "deemed exports" when released to a foreign national and are controlled. [67] This further demonstrates the lack of continuity throughout the federal government regarding the restrictions and/or publications of certain data that may prove harmful to the national security. This makes it especially difficult for those attempting to obtain the necessary permissions for sharing technical data across multiple university campuses or business partners' campuses overseas. This can be very detrimental to ongoing research and development of technical projects, ironically even to those who seek to further the protection afforded the national security. Of course, the research itself may also threaten national security.

More on Classification

Initial efforts to maintain secrecy were conducted voluntarily. During the research on the Manhattan Project, the physicists involved voluntarily stopped publishing results to keep from aiding the German nuclear bomb development efforts. [68] Later, a National Academy of Sciences-National Research Council Advisory Committee on Scientific Publications was established to restrict publication regarding nuclear fission. [69] There have been further delineations of restrictions on nuclear information, as previously mentioned, as specified in the Atomic Energy Act of 1954. This further explanation and redefinition allowed for more research into the development of atomic power, while at the same time further restricting access to information regarding atomic weapons, special nuclear material, and/or the development of special nuclear material. [70]

Currently, not only information related to nuclear power, but all sensitive information is covered by National Security Decision Directive 189 (NSDD-189). [71] This was signed by then President Ronald Reagan in 1985. This directive stated the following:

> It is the policy of this Administration that, to the maximum extent possible, the products of fundamental research remain unrestricted. It is also the policy of this Administration that, where the national security requires control, the mechanism for control of information generated during federally-funded fundamental research in science, technology and engineering at colleges, universities and laboratories is classification. Each federal government agency is responsible for: a) determining whether classification is appropriate prior to the aware of a research grant, contract, or cooperative agreement and, if so, controlling the research results through standard classification procedures; b) periodically reviewing all research grants, contracts, or cooperative agreements for potential classification. No restrictions may be placed upon the conduct or reporting of federally-funded fundamental research that has not received national security classification, except as provided in applicable U.S. Statutes. [72]

Further, fundamental research is also defined within NSDD-189 as:

> "Fundamental research" means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons. [73]

This NSDD has not been superceded and thus continues to be current policy. Recently, this position has been reaffirmed by a letter from Condoleezza Rice, Assistant to the President for National Security Affairs, to Dr. Harold Brown, co-Chairman of the Center for Strategic and International Studies. In part, this letter stated:

> …this Administration will review and update as appropriate the export control policies that affect basic research in the United States. In the interim, the policy on the transfer of scientific, technical, and engineering information set forth in NSDD-189 shall remain in effect… [74]

However, the Bush administration has not been silent following the terrorist attacks on the United States in September of 2001. In addition to reaffirming NSDD 189, President Bush's administration has amended Executive Order 12958, Classified National Security Information of April 17, 1995, with Executive Order 13292 on March 15, 2003. E.O. 12958 permitted classification of "scientific, technological, or economic matters relating the national security" in Section 1.5. Section 1.8(b) forbade classification of " basic scientific research information not related to the national security." [75] The amendment by E.O 13292 added a clause to section 1.5, permitting classification of "scientific, technological, or economic matters relating to the national security, **which**

includes defense against transnational terrorism" (emphasis added). [76] Transnational terrorism seems to be another deliberately vague term, as it is not further defined. (Please see Appendix D for one definition of transnational terrorism.) Given this description, the federal government seems to possess wide latitude in declaring information, even purely scientific research, classified or at least sensitive to prevent publication.

Pre-Publication Review

Even given the recent changes to federal policies, most scientific research is not encumbered by lack of publication. However, there is a burden on the scientific research community. They must submit their information to appropriate agencies for "pre-publication review." [77] The government will review even some "privately published scientific and technical data by current and former employees and contractors who worked for federal agencies and who had access to classified information." Among other agencies who conduct this review, the Department of Agriculture has issued the following guidance:

> In order to protect against the unauthorized disclosure of classified information, you are required to submit for security review any material intended for public release that might be based in any way on information you learned through your access to classified information. This requirement covers all written materials, including technical papers, books, articles, and manuscripts. It also includes lectures, speeches, films, videotapes. It includes works of fiction as well as non-fiction. [78]

Other agencies include pre-publication review as part of federal contracts. The Department of Defense includes this clause in contracts for extramural research that allows it to review any research generated with federal support prior to publication. Likewise, information generated by research conducted on classified information or when information is considered sensitive because of the way it is compiled.

Additionally, the National Security Agency performs a pre-publication review of all academic cryptography research. This research is submitted voluntarily by agreement with the American Council on Education. [79] The government also has the ability to sign exclusive contracts with providers of commercial satellite imagery and to stop the collection and dissemination of commercial satellite imagery for national security reasons. [80]

Additional Controls

There are some additional controls placed on the potential dissemination of information, specifically concerning biomedical research. These controls were instituted by the USA Patriot Act, P.L. 107-56, and the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, P.L. 107-188, also the

Agricultural Bioterrorism Protection Act of 2002, (part of) P.L. 107-56. These acts placed limits on public access to "certain biological agents and toxins". [81] Prior to these acts, any US laboratory that transported "select agents" (a list of about 40 dangerous biological agents and toxins) had to register with the government. (See 42 CFR 72.6) Following the passage of the aforementioned acts, the list has expanded to about 60 select agents that could be use to commit bioterrorism. [82]

Pursuant to these laws, the laboratories that use the agents listed therein must register and control access to these agents. Further, the scientists will have to register, submit to background checks, and obtain prior approval to use, send, or receive select agents used in experiments. Even research conducted by privately-funded organizations will have to comply with these rules and receive "prior approval from the Department of Health and Human Services." [83] These acts provide for civil and criminal penalties for non-compliance. All laboratories that handle these select agents will have to be in compliance with these laws by fall 2003.

SENSITIVE BUT UNCLASSIFIED

The widest "category" of protected information is the so-called "sensitive but unclassified." This information is defined generally by various presidential-level directives and agency guidelines. Different government agencies have interpreted the meanings differently. There does not seem to be a consensus amongst the various departments. Some agencies use the terms "for official use only," "limited use," "sensitive," "sensitive but unclassified" and others interchangeably. Generally, sensitive but unclassified has been defined by the following acts: Privacy Act of 1974 (5 USC 552a), the Freedom of Information Act (FOIA) of 1966 (5 USC 552), the Computer Security Act of 1987 (relevant portions codified at 15 USC 278 g-3), and others. Agencies understand that each is to interpret the language of the acts to protect their sensitive information. Each agency has provided for various criminal and civil penalties for releasing sensitive but unclassified information. See Appendix A for the full description of the history of sensitive but unclassified.

There is no agreement among various governmental agencies regarding a uniform definition of "sensitive but unclassified" or the ways to ensure the protection of such information. [84] The positions of certain government agencies are outlined below.

State Department

In the Foreign Affairs Manual, of October 1995, the State Department stated it would no longer use the designation "limited official use" but would begin using Sensitive But Unclassified (SBU) for information exempt from FOIA disclosure. [85] The manual further stated:

> a. SBU describes information which warrants a degree of protection and administrative control that meets the criteria for exemption from public disclosure set forth under Sections 552 and 552a of Title 5, United States Code: the Freedom of Information Act and the Privacy Act. [86]

The State Department has also said

> b. SBU information includes, but is not limited to: (1) Medical, personnel, financial, investigatory, visa, law enforcement, or other information which, if released, could result in harm or unfair treatment to any individual or group, or could have a negative impact upon foreign policy or relations; and (2) information offered under conditions of confidentiality which arises in the course of a deliberative process (or a civil discover process), including attorney-client privilege or work product, and information arising from the advice and counsel of subordinates to policy makers. [87]

The State Department sent a telegram to U.S. embassies explaining "sensitive but unclassified is not a classification level for national security information, but is used when it's necessary to provide a degree of protection from unauthorized disclosure for unclassified information as set forth in 12 FAM 540." [88] Further, they stated "public access to SBU information would be limited to those with a need to know and would be subject to provisions which govern disclosure and exemptions in the FOIA". [89]

The Defense Department

The Department of Defense issued guidance for "controlled unclassified information" in 1997 stating that "For Official Use Only" (FOUO) should be used for unclassified information needing protection from public release. [90] This was to include the former Limited Office Use and sensitive but unclassified designations. The DoD further stated "there must be a legitimate Government purpose served by withholding it". [91] See also Guidance for Telework Involving Sensitive-Unclassified information, prepared by Naval Air Warfare Center Aircraft Division, http://hro.navair.navy.mil/telework/sensunclass.htm.

The same DoD directive limited dissemination of FOUO information to:

> … within the DoD Components and between officials of the DoD Components and DoD contractors, consultants and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. (Special restrictions may apply to information covered by the Privacy Act.) Release of FOUO information to Members of Congress is

> covered by DoD Directive 5400.4, and to the General Accounting Office by DoD Directive 7650.1. [92]

Army Regulations, specifically 380-19, Section 1-5 provides examples of some SBU information

> that: (a) involves intelligence activities, (b) involves cryptological activities related to national security, (c) involves command and control of forces, (d) is contained in systems that are an integral part of weapon or a weapon system, (e) is contained in systems that are critical to the direct fulfillment of military or intelligence missions, (f) involves processing of research, development, and engineering data."[93]

Further, the Army states the obvious: "Other factors such as risk management … should be taken into account". They state the ultimate decision of the sensitivity of the data should be determined by the owner/creator of the data. [94]

SBU Matrix

The following is an excerpt from the same Smith document, at Page 13, entitled "SBU Matrix".

The matrix below provides a general guide on the data categories and description of the types of data that should be considered Sensitive But Unclassified. [95] This matrix should not be considered authoritative or all-inclusive.

Data Category	Description
FOIA Exempted	Any information that is exempted from mandatory disclosure under the Freedom of Information Act.
Intelligence Activities	Information that involves or is related in intelligence activities, including collection methods, personnel, and unclassified information.
Cryptologic Activities	Information that involves encryption/decryption of information; communications security equipment, keys, algorithms, processes; information involving the methods and internal workings of cryptologic equipment.
Command and Control	Information involving the command and control of forces, troop movements.
Weapon and Weapon Systems	Information that deals with the design, functionality, and capabilities of weapons and weapon systems both fielded and un-fielded.
RD&E	Research, development, and engineering data on un-fielded products, projects, systems, and programs that are in the development or acquisition phase.
Logistics	Information dealing with logistics, supplies, materials, parts and parts requisitions, including quantities and

	numbers.
Medical Care/HIPAA	Information dealing with personal medical care, patient treatment, prescriptions, physician notes, patient charts, x-rays, diagnosis, etc.
Personnel Management	Information dealing with personnel, including evaluations, individual salaries, assignments, and internal personnel management.
Privacy Act Data	Information covered by the Privacy Act of 1974 (5 U.S.C. § 552A)
Contractual Data	Information and records pertaining to contracts, bids, proposals, and other data involving government contracts.
Investigative Data	Information and data pertaining to official criminal and civil investigations such as investigator notes and attorney-client privileged information.

Department of Energy

The Department of Energy uses the exact definition of Sensitive But Unclassified as outlined in the Poindexter document of 1986. That definition is:

> Sensitive Unclassified Information: Information for which disclosure, loss, misuse, alteration, or destruction could adversely affect national security or governmental interests. National security interests are those unclassified matters that relate to the national defense or foreign relations of the U.S. Government. Governmental interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law-enforcement information, as well as the privacy or confidentiality of personal or commercial proprietary information provided to the U.S. Government by its citizens. [96]

Other Agencies

Other agencies have provided additional definitions of SBU. In 2002, the General Services Administration (GSA) included in their definition of SBU "information that could possibly benefit terrorists, such as equipment plans, building designs, operating plans, the locations of secure facilities or functions within GSA buildings, utility locations, and information about security systems or guards." [97]

The Federal Aviation Administration (FAA) has delineated regulations to protect unclassified but

> 'sensitive security information' which may be developed from security or research and development activities and whose release, the Administration determines, could be an invasion of personal privacy, reveal private or financial information, or could "be detrimental to the safety of passengers in transportation". [98]

Finally **NASA** (National Aeronautics and Space Administration) defines unclassified sensitive information as "administrative controlled information (ACI)", and sets forth instructions for handling this information under the same heading as controlling classified national security information (CNSI):

> Such information and material, which may be exempt from disclosure by statute or is determined by a designated NASA official to be especially sensitive, shall be afforded physical protection sufficient to safeguard it from unauthorized disclosure. Within NASA, such information has previously been designated "For Official Use Only". [99]

Demonstrably, there is no agreement regarding the definition of sensitive but unclassified. All agencies seem to not only utilize the definition provided by the Card Memorandum, but seem to include information exempted from FOIA production as well as information considered by the Computer Security Act of 1987. Please remember that each agency has also been given discretion under FOIA to secure sensitive information. [100]

SENSITIVE VERSUS SENSITIVE BUT UNCLASSIFIED

Incredibly, the government says there is a difference between sensitive information, and sensitive but unclassified. According to guidance issued by the Navy by 1997, the Computer Security Act of 1987 defined requirement for "sensitive but unclassified" information and further stated "all business conducted within the federal government is sensitive but unclassified." [101]

A year later, in 1998, the similarities between sensitive and sensitive but unclassified was codified by DOD in administrative law at 32 CFR 149.3, specifically relating to technical surveillance countermeasures used by all federal agencies that process SBU. [102] The DoD used the definition of sensitive that appeared in the Computer Security Act of 1987 to define sensitive but unclassified. [103]

Even the Department of the Interior had a separate definition of SBU – "all unclassified DOI systems are considered SBU." [104]

THE CARD MEMO

In March 2002, Andrew Card, the White House Chief of Staff, issued a memo entitled "Action to Safeguard Information Regarding Weapons of Mass

Destruction and Other Sensitive Documents Related to Homeland Security." This memo instructed government agencies to reconsider their current policies for protection sensitive information regarding weapons of mass destruction and "other sensitive documents related to homeland security and 'information that could be misused to harm the security of our Nation and the safety of our people'." [105] See Appendix B for the entire text of the memo. Agencies were expected to review their policies in accordance with memos by the National Archives and Records Administration (NARA) Information Security Oversight Office (ISOO) attached to the Card memo and report their findings to the Office of Homeland Security within 90 days (White House Memorandum for the Heads of Executive Departments and Agencies From Andrew H. Card, Jr., The White House, Subject: "Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security," March 19, 2002. Source: http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm).

The NARA memo attached to the Card memo had a section titled "Sensitive But Unclassified information" (SBU) instructing agencies to protect "sensitive information related to America's homeland security" (SHSI). [106] This memo further instructed agencies to consider all applicable FOIA exemptions if FOIA requests are received. [107] Please see Appendix C for the full text of the Freedom of Information Act, including the exemptions, especially 2 and 4. Exemptions 2 and 4 to the FOIA are generally used to deny FOIA request for SBU.

As still further guidance, NARA referred back to additional direction from Attorney General John Ashcroft issued in October 2001. This memo directed agencies to "consider protecting values and interests to which the Administration is committed, including 'safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information, and, not least, preserving personal privacy'." [108]

In previous direction, agencies had been encouraged to release documents even if the law provided for withholding them, if there was no "foreseeable harm" in doing so. [109] This memo encouraged agencies to disclose information "only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information."

Additionally, the memo told agencies to utilize FOIA exemption 2 "to protect critical infrastructure information", referenced in the memo as "critical systems, facilities, stockpiles, and other assets from security breaches and harm." [110] Unnecessarily, the memo included the need for "protection of any agency information that could enable someone to succeed in causing the feared harm" (Ibid). The memo further instructed agencies to "avail themselves of the full measure of exemption 2's protection for their critical infrastructure information as they continued to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks". [111]

The Bush Administration's position on SBU seems to include information dealing with the agency, public infrastructure the agency regulations or monitors, some internal databases, vulnerability assessments, some internal deliberations, and information provided to the government by private firms, such as chemical companies. [112]

In November 2002, the Department of Homeland Security Act, P.L. 107-296, was passed. This law prohibited disclosure of "critical infrastructure information" under FOIA request. It provides for fines, dismissal or imprisonment for up to a year for violators (Section 214). [113]

POLICY ISSUES REGARDING SBU

As previously mentioned, most government agencies have used a combination of the definition of SBU provided in the Computer Security Act of 1987 and other directives. After the September 11, 2001 terrorist attacks, the Bush Administration advised agencies responding to FOIA requests to balance the release of information with the need to protect critical infrastructure information and national security, and specifically to use FOIA exemptions 2 and 4.

However, in this precarious balancing attempt, some believe the administration has sought too great a limit on the release of information. Some say the terms "Sensitive" and "SBU" are not properly defined and allow for too wide a range of interpretation. [114] Of course, one of the easiest arguments to make is the lack of uniformity in the standards of what constitutes SBU from agency to agency. It really is the age old struggle between those who do not wish to provide any information to the public and those who advocate an entirely open government with free access to everything.

Historical Controversy Over SBU

Years before the September 11 attacks, there had already been discussions regarding vague definition(s) of SBU. As there are two sides to every argument, the opinions fall into two camps. One side claims SBU should be interpreted broadly to safeguard more information. The other side believes the designation is overly vague and allows the withholding of too much information.

In February 1994, in a report prepared for the Secretary of Defense and the Director of the CIA, the Joint Security Commission (JSC) estimated that "as much as 75% of all government-held information could be sensitive and unclassified". [115] The JSC recommended protecting more information pertaining to the defense, intelligence and other sectors. They further stated that this information "is crucial to the U.S. security in its broadest sense". They went on to say:

> 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 communications networks, and the power grids and pipeline networks. All of these are highly automated systems that require appropriate security measures to protect confidentiality, integrity and availability. [116]

On the opposite side, the Moynihan commission report (Report of the Commission on Protecting and Reducing Government Secrecy, 1997) cited the discrepancies in the various agencies' handling of SBU. The report claimed this created problems because:

> … virtually any agency employee can decide which information is to be so regulated;" there is no oversight of this categorization and agencies control access "through a need-to-know process," and "… the very lack of consistency from one agency to another contributes to confusion about why this information is to be protected and how it is to be handled. These designations sometimes are mistaken for a fourth classification level, causing unclassified information with these markings to be treated like classified information. [117]

The Moynihan report clearly believed that more information should be released. They stated that efforts had been made in 1994 to clearly define SBU but that it had "met with great resistance by both the civilian side of the Government and industry." They claimed this was because the controlling agency, the Security Policy Board, was controlled by the defense and intelligence communities. [118]

In a critique of the DOE definition of SBU, the Center for Strategic and International Studies (CSIS) complained: "The Department's official definition is so broad as to be unusable". [119] They further stated the DOE had no meaningful, consistent control over SBU and could not agree on what significance protecting this information had for U.S. national security.

The major complaint has always been that by designating information as SBU, it practically adds a fourth classification. The CSIS commission suggested the DOE refrain from labeling information SBU. It recommended the Department

> should have just three classes of information: (1) classified; (2) unclassified but subject to administrative controls; and (3) unclassified, publicly releasable." (Science and Security in the 21st Century, op. cit., p. 62) They further recommended the DOE utilize the "Official Use Only" designation for any sensitive information that did not attain the level of classified. [120]

Official Use Only information is defined: "A designation identifying certain unclassified but sensitive information that may be exempt from public release

under the FOIA from DOE 471.2A. [121] OUO is administered within a single office in DOE, which has guidelines established in law and unclassified information could be reviewed for applicability under the OUO statutes.

The Card memo has likewise been criticized. In "Making Sense of Information Restrictions After September 11," Steven Aftergood and Henry Kelly stated "several of the new restrictions on information are not congruent with the existing legal framework defined by the Freedom of Information Act (FOIA) or with the executive order (Executive Order 12598) that governs National Security classification and declassification." [122]

Concerns About Sensitive Information

Some have argued that government agencies should make no provision for SBU. They claim that implementing policy for protecting SBU by presidential directives or agency regulations fails to attain the level of previously codified statutes, which are silent. CRS-31. It has been argued that SBU may be "the most dangerous level of secrecy, because it was not defined [in the past] and there were no channels of appeal." [123] And this has been true in the past. Now, the standard seems to be better defined although the definition seems to vary from agency to agency. The government still should provide a remedy or review for those who disagree with the withholding information based on the SBU designation. [124]

Of course, some information probably should not be freely available regardless. In a perfect world, it would be great to be able to publish everything. But in today's world, withholding of some information seems to be for the public good. The National Academy of Sciences voluntarily removed information regarding vulnerabilities of croplands from a report prepared for the U.S. Department of Agriculture because of concerns terrorists might be able to exploit the vulnerabilities highlighted within. [125]

The remedy adopted by the NAS seems to be a fair blueprint that the Government would do well to duplicate. If someone should wish to obtain a copy of the information that was removed from the report and placed under separate cover, he must file a written request. The person making the request will then be called to verify the application, have their identity verified, and then questioned as to why they need the information. [126] Presumably anyone who has been verified and can demonstrate a need for the information will be provided the information.

This policy seems to have only mildly satisfied those who believe in open government. In October 2002, the presidents of the National Academies issued a statement ("Presidents Statement on Science and Security in an Age of Terrorism, From Bruce Alberts, William A. Wulf, and Harvey Fineberg, Presidents of the National Academies," October 18, 2002) seeking to balance security and openness in disseminating scientific information. They summarized as follows:

"Restrictions are clearly needed to safeguard strategic secrets; but openness also is needed to accelerate the progress of technical knowledge and enhance the nation's understanding of potential threats." In their statement, they further urged agencies to not use SBU, claiming "experience shows that vague criteria of this kind generate deep uncertainties among both scientists and officials responsible for enforcing regulations. The inevitable effect is to stifle scientific creativity and to weaken national security." It seems our national academies recognize there is a need for security, but they do not believe any "scientific research" should be protected. [127]

In 2003, the National Academies held a workshop in conjunction with the CSIS. Administration officials attended and suggested the scientists develop their own voluntary policy and assist the Administration in protecting "truly sensitive findings." [128] Both the Academies and CSIS continue to cooperate in their efforts to craft this policy.

Those working in microbiology seem to agree with the premise that research should be open, but also seem to have a better recognition of the potential harm of their research. They have stated "that while transparency in publication should be the norm, consideration should be given to developing a 'specially appointed committee to determine whether publication is appropriate'." [129]

Even librarians have something to say. In June 2002, the Council of the American Library Association adopted a resolution urging that the provisions relating to SBU be dropped from the Card memo and urged "government agencies … ensure that public access to government information is maintained absent specific compelling and documented national security or public safety concerns." [130]

Government Efforts

In 2002, Congressman Dave Weldon (R-FL) introduced House Resolution 514 to urge the scientific community to ensure that information that may be used by terrorists is not made widely available, or is properly classified. [131] Unfortunately, the resolution never made it out of committee.

In testimony given during hearings on *Conducting Research During the War on Terrorism: Balancing Openness and Security*, the Director of the White House Office of Science and Technology, John Marburger testified the Administration seeks "to ensure an open scientific environment" while maintaining homeland security. He stated that sensitive but unclassified homeland security information guidelines would apply to intelligence and public health information, but not necessarily to research. [132]

POLICY OPTIONS

Clearly defining protective yet open policy regarding SBU is a difficult matter. As has been outlined in these pages previously, there is a vast difference of opinion in society and even amongst various government agencies. However, the Administration must not shrink from this responsibility. Initial steps should focus on creating a consensus among the various governmental agencies as to an appropriate definition of SBU.

The responsibility clearly lies with the President under P.L. 107-296, the Homeland Security Act. This law requires research conducted by the Department of Homeland Security "shall be unclassified to the greatest extent possible". However, the President has stated his intent to protect information "which could otherwise harm the foreign relations or national security of the United States." [133]

Uniform Definition of Sensitive But Unclassified

Without a clear policy regarding the definition of SBU, none of the various governmental agencies can be reasonably expected to agree on what information can or should be released to the public. It is currently open to subjective interpretation by various employees working in the agencies and what these employees believe may be of value to terrorists. This should not be the case much longer. At the request of the Office of Homeland Security, the White House Office of Science and Technology Policy and the Office of Management and Budget are working together to develop guidelines for SBU. Hopefully, we will have a well-defined policy in regards to SBU following the completion of their work. [134]

Presently, the various agencies have discretion to identify and withhold from the public information they determine is subject to either nondisclosure agreements or FOIA exemptions. We've previously defined, ad nauseum, what could be considered sensitive information by the various acts, so we won't discuss that again. But to consider for a moment what might actually go into this policy, let's look at what else the Administration has said.

The Administration has instructed agencies to carefully consider their response to requests for information. They have been urged to consider the "need to protect critical systems, facilities, stockpiles, and other assets from security breaches and harm – and in some instances from their potential use as weapons of mass destruction in and of themselves. [135] Further, agencies have also been urged to apply exemptions 2 and 4 when responding to FOIA requests, considering the needs for informed citizens, and "safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information, and not least preserving personal privacy." [136]

The Administration seems to support restricting more information that might have previously been accessible to the public, where that information may be harmful to national security. The objective seems clear, to withhold information when there is no "need to know", but allow access to it for appropriate personnel. [137] This is an admirable and proper objective, and with luck and intelligence, will be adopted and implemented soon.

To further the protection of sensitive information, the Administration has granted additional agency heads original classification authority. These include the Secretary of Health and Human Services, the Secretary of Agriculture, and the Administrator of the Environmental Protection Agency. [138] With the additional authority or original classification now resting with these agency heads, there is potential that a large group of information not previously classified may become classified. It is obvious that these agencies possess information that may be of some value to those wishing to create calamity amongst the masses.

Again, the Administration seems to support more classification. Executive Order 13292, which amended E.O. 12958 on classified national security information, permits the classification of "scientific, technological, or economic matters relating to the national security, *which includes defense against transnational terrorism*" (new text in italics).

What seems to be unclear is whether or not the Administration truly intends that more information be classified. The definition of national security remains the same in both Executive Orders. The amended Executive Order merely adds the phrase regarding transnational terrorism.

Various governmental agencies are expected to continue the policy of pre-publication review discussed earlier. It would not be surprising for each agency to issue guidelines clarifying the treatment of questionable information. Given the traditional position of the government to release basic scientific research provided it doesn't threaten national security, the balance between releasing information and protecting information will surely remain a closely watched subject.

Appeals Process

As stated previously, to provide a remedy to challenge the designation of sensitive but unclassified, an appeals process should be implemented. This process has long been followed and can be demonstrated by an executive branch body called the Interagency Security Classification Appeals Panel (ISCAP). [139] It has been suggested the membership of this appeals panel should be drawn from agencies outside the originating agency to prevent any undue influence and enhance the credibility of the process. It has also been suggested that the Information Security Oversight Office provide an appeals review. [140] Either way, a third party review might allow for greater openness and more

effective protection. It may also provide an avenue for creating compromise acceptable to all.

Federal Agency Action

Shortly after the issuance of the Card memo, agencies began to remove information that was previously available. This information was either previously available online or in public libraries. [141] It is said that the DOE "removed environmental impact statements which alerted local communities to potential dangers from nearby nuclear energy plants, as well as information on the transportation of hazardous materials". [142]

According to a published report, the EPA has removed documents from its website and the DOD has pulled more than 6000 documents. [143] Please see http://tigger/uic/edu/~tfontno/chr.html for a list of "disappearing information."

Some expect less information to be made available because of passage of the Homeland Security Act. While most agree this provides needed protection for potential vulnerabilities to critical infrastructure, some fear "that companies could ensure secrecy for a wide range of information provided to the government simply by declaring that it involves critical infrastructure and then demanding confidentiality." [144] These same groups contend that the law might "prevent the disclosure of potential health risks from uranium stored at private sites or of defects in railroad tracks … [or] … that the law might discourage whistle-blowers from coming forward with revelations about corporate wrongdoing." [145] Of course, these are the same people who have filed a lawsuit "against the Patriot Act". [146]

"Tiered" Access to SBU

There has been discussion of pre-qualifying individuals to access a certain level or tier of sensitive information. This would allow those individuals who regularly require access to scientific and/or technical information throughout the government and private industry easier access while at the same time providing protection for sensitive information. A form of this is already practiced by the EPA. [147] It is good that the EPA intends to keep sensitive information safe, as they have called for all utilities to submit threat or vulnerability assessment to the agency." [148] Additionally, FERC (Federal Energy Regulatory Commission) has proposed limiting access to its critical energy infrastructure information on a tiered basis. [149] Similarly, the U.S. Geological Survey has said it will implement four levels of control for its information. [150]

Conclusions

While all of this proposed levels of access, creation of a review process, and further definition of sensitive but unclassified information provides a good framework, I expect there will be ongoing debate. This will remain a

controversial issue until it is codified, and may remain so even after becoming law. But we cannot allow the controversial nature of protecting information versus free and open access to everything to keep us from our duty.

In order to maintain this safety and security of all our citizens, we must all do our part. Government and Private Industry must make a concerted effort to work more closely together. Everyone who posts information to a website, or publishes information in magazines or books, must review this information with a more critical eye towards possible harmful uses. Information must be reviewed that is currently available to determine if it is sensitive. This must be a continuous process of reviewing information and ensuring compliance. Remember, "stupidity trumps security." [151]

We must not allow our freedoms to become a threat. And we, on the information frontlines, must remember that our work has real world implications. We cannot become a tool that terrorists use to obtain cyber information to enable physical attacks.

ENDNOTES

1 – The National Strategy to Secure Cyberspace. February 2003. 12

2 – Verton, Dan. "Web sites seen as terrorist aids." Computerworld. February 11, 2002. URL: http://www.computerworld.com/industrytopics/energy/story/0,10801,68181,00.html (August 22, 2003).

3 – Ibid.

4 – Ibid.

5 – "Maps of Nuclear Power Reactors: World Map." International Nuclear Safety Center. URL: http://insc.anl.gov/pwrmaps (August 15, 2003).

6 – URL: http://www.terraserver-usa.com/ (August 15, 2003).

7 – "Nuclear Waste Transportation Routes". Agency for Nuclear Projects. URL: http://www.state.nv.us/nucwaste/states/us.htm (August 15, 2003).

8 - 'Electric Power Information Assurance Risk Assessment', The President's National Security Telecommunications Advisory Committee, Information Assurance Task Force, March 1997

9 – Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." SecurityFocus. Aug. 19, 2003, http://www.securityfocus.com/news/6767 (August 19, 2003).

10 – Kozlow, Christopher and Sullivan, John, Jane's Facility Security Handbook, Alexandria: Jane's Information Group, June 2000. 5

11 – Ibid

12 – Evans, Noell Wolfgram. "Trick or Treat and Halloween History." 2002. URL: http://ky.essortment.com/halloweenhistor_ryqj.htm (August 25, 2003).

13 – Verton, Dan. "U.S. Infrastructure Shaken By Terrorist Attack." Computerworld. September 11, 2001. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,63719,00.html (August 18, 2003).

14 – Associated Press. "Web sites remove data, citing security concerns in wake of attacks." October 4, 2001. URL: http://www.freedomforum.org/templates/document.asp?documentID=15066 (August 1, 2003).

15 – “California Energy Maps.” Map of Power Plants in California. June 26, 2003. URL: http://www.energy.ca.gov/maps/power_plant.html (July 8, 2003).

16 – “California Energy Maps.” California’s Major Electric Transmission Lines. September 6, 2000. URL: http://www.energy.ca.gov/maps/transmission_lines.html (July 8, 2003).

17 – Blumenfeld, Laura. “Dissertation Could Be Security Threat.” Washington Post. July 8, 2003. URL: http://www.washingtonpost.com/ac2/wp-dyn/A23689-2003Jul7?language=printer (July 31, 2003).

18 – Moteff, John, Copeland, Claudia, and Fischer, John. “Critical Infrastructures: What Makes an Infrastructure Critical?” Report for Congress. Order Code RL31556: CRS-1.

19 – Glossary. “State Infrastructure Protection Advisory Committee.” Office of the Attorney General, State of Texas. URL: http://www.oag.state.tx.us/sipac/glos_acro.htm (August 15, 2003).

20 – “Protecting the Nation’s Infrastructure”. Heritage Foundation Report on Infrastructure Protection. January 8, 2002. URL: http://www.itsa.org/itsnews.nsf/0/752ad9b60686c4a085256b3d004163d?opendocument (August 15, 2003).

21 – “The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 663”. White Paper. May 22, 1998. URL: http://www.fas.org/irp/offdocs/paper598.htm (August 25, 2003).

22 – Executive Order *13228 – Establishing the Office of Homeland Security and the Homeland Security Council*. Federal Register, Vol. 66, No. 196. October 8, 2001: pp. 51812-51817.

23 – “The Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 663”. White Paper. May 22, 1998. URL: http://www.fas.org/irp/offdocs/paper598.htm (August 25, 2003).

24 – Moteff, John, Copeland, Claudia, and Fischer, John. “Critical Infrastructures: What Makes an Infrastructure Critical?” Report for Congress. Order Code RL31556: CRS-8.

25 – “Make IT Governance an Integral Part of the Enterprise”, Alexander J. Breeding, June 16, 2003, CNET Networks, http://techrepublic.com.com/5100-6298-5035046.html?tag=search

26 – "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 663". White Paper. May 22, 1998. URL: http://www.fas.org/irp/offdocs/paper598.htm (August 25, 2003).

27 – Deutch, John M. "Foreign Information Warfare Programs and Capabilities". Taken from Central Intelligence Agency Speeches and Testimony. June 25, 1996. URL: http://www.cia.gov/cia/public_affairs/speeches/1996/dci_testimony_062596.html (July 28, 2003).

28 – Ibid

29 – Ibid

30 – Verton, Dan. "U.S. Infrastructure Shaken by Terrorist Attack." Computerworld. September 11, 2001. URL: http://www.computerworld.com/securitytopics/security/story/0,10801,63719,00.html (August 18, 2003).

31 – Borland, Jerry. "WTC Disaster Causes Extensive Damage to Electric Infrastructure." PowerQuality. September 14, 2001.

32 – Executive Order *13228 – Establishing the Office of Homeland Security and the Homeland Security Council*. Federal Register, Vol. 66, No. 196. October 8, 2001. pp. 51812-51817.

33 – ibid.

34 – Executive Order *13231 – Critical Infrastructure Protection in the Information Age*. Federal Register, Vol. 86, No. 202. October 18, 2001. pp. 53063-53071.

35 – ibid.

36 – USA Patriot Act (P.L. 107-56). October 26, 2001.

37 – National Strategy for Homeland Security. July 2002. p. 42

38 – Malveaux, Suzanne. "Bush: Blackout is 'Wake-Up' Call". cnn.com. August 15, 2003. URL: http://www.cnn.com/2003/allpolitics/08/15/bush.blackout/index.html. **See also**, Associated Press, "Planes, Trains Recovering from Blackout". cnn.com. August 15, 2003. URL: http://www.cnn.com/2003/travel/08/15/air.traffic.ap/index.html; Botelho, Greg. "Lights Returning in Power Grid-Lock". cnn.com. August 15, 2003. URL: http://www.fox11az.com/news/other/stories/kmsb_local_power_081503.b6a7206.html; Kehnemui, Sharon. "Massive Blackout Cripples Northeast". Foxnews.com.

August 14, 2003. URL:
http://www.foxnews.com/printer_friendly_story/0,3566,94772,00.html

39 – National Research Council. Transportation Research Board. TRB Special Report 270. *Deterrence, Protection, and Preparation – The New Transportation Security Imperative*. July 2, 2002.

40 – Moteff, John, Copeland, Claudia, and Fischer, John. "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress. Order Code RL31556: CRS-8.

41 – Moteff, John, Copeland, Claudia, and Fischer, John. "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress. Order Code RL31556: CRS-9.

42 – Romeo, Jessica. "New Risks and Realities." Security Now. Business 2.0. April 2002. URL:
http://www.fortune.com/fortune/services/sections/fortune/tech/2002_04securityBusiness2.html (August 25, 2003).

43 – "Cyber Security of the Electric Power Industry." Institute for Security Technology Studies at Dartmouth College. December 2002.
http://www.ists.dartmouth.edu/ISTS/ists_docs/cselectric.pdf (August 25, 2003).

44 – "Pennsylvania Environmental Network Green Energy Leadership Team." URL: http://www.penweb.org/issues/energy/ (August 25, 2003).

45 – Blumenfeld, op. cit.

46 – "Rethinking Classification: Better Protection and Greater Openness." Report of the Commission on Protecting and Reducing Government Secrecy. URL:
http://www.dss.mil/seclib/govsec/chap2.htm (July 28, 2003): p. 6.

47 – "Rethinking Classification: Better Protection and Greater Openness." Report of the Commission on Protecting and Reducing Government Secrecy. URL:
http://www.dss.mil/seclib/govsec/chap2.htm (July 28, 2003): p. 1.

48 – White House, Office of the President, *National Security Decision Directive 189*. September 21, 1985. URL: http://www.aau.edu/research/ITAR-NSDD189.html (August 25, 2003)

49 – Executive Order *12958 – Classified National Security Information*. Federal Register, Vol. 60, No. 76. April 20, 1995. p. 19825.

50 – Memorandum for the Heads of Executive Departments and Agencies, From: Andrew H. Card, Jr., Assistant to the President and Chief of Staff, Subj: Action to

Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security. March 19, 2002. URL: http://www.fax.org/sgp/bush/wh031902.html (August 15, 2003).

51 – ibid.

52 – Knezo, Genevieve J. "'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy." April 2, 2003: 17.

53 – Knezo, op. cit., p. 20.

54 – Knezo, op. cit., p. 18.

55 – Graham, Mary. "The Information Wars." The Atlantic Monthly. September 2002. pp. 36-38.

56 – Alberts, Bruce, Wulf, William A., and Fineberg, Harvey, Presidents of the National Academies. "Statement on Science and Security in an Age of Terrorism." October 18, 2002.

57 – Miller, Barbara. "Chronology of Disappearing Government Information." October 31, 2002. URL: http://tigger/uic/edu/~tfontno/chr.html (July 31, 2003).

58 – Machlis, Sharon. "Update: Microsoft.com Hit By DOS Attack." Computerworld. August 1, 2003. URL: http://www.computerworld.com/developmenttopics/websitemgmt/story/0,10801,83677,00.html?nas=SEC-83677 (August 25, 2003).

59 – The Freedom of Information Act. 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048.

60 – 35 U.S.C. §§ 181-188.

61 – Knezo, op. cit., 2.

62 – "Rethinking Classification: Better Protection and Greater Openness." Report of the Commission on Protecting and Reducing Government Secrecy. URL: http://www.dss.mil/seclib/govsec/chap2.htm (July 28, 2003): p. 5.

63 – ibid.

64 – 42 U.S.C. § 2162

65 – 15 CFR § 772.1

66 – 22 CFR § 120.11

67 – 15 CFR § 734.2(b)

68 – Westwick, Peter J. "In the Beginning: The Origin of Nuclear Secrecy," *Bulleting of the Atomic Scientists*, Vol. 56, (November/December 2000), pp. 43-49.

69 – Cochrane, Rexmond C. The National Academy of Sciences: The First Hundred Years, 1863-1963, (Washington, D.C.: National Academy of Sciences), 1978, pp. 385-387

70 – The Atomic Energy Act of 1954

71 – White House, Office of the President, *National Security Decision Directive 189*. September 21, 1985. URL: http://www.aau.edu/research/ITAR-NSDD189.html (August 25, 2003)

72 – ibid.

73 – ibid.

74 – Rice, Condoleeza, Assistant to the President for National Security Affairs. Letter to Dr. Harold Brown, co-Chairman, Center for Strategic and International Studies, November 1, 2001.

75 – Executive Order *12958 – Classified National Security Information*. Federal Register, Vol. 60, No. 76. April 20, 1995. p. 19825.

76 – Executive Order *13292 – Further Amendment to Executive Order 12958, as Amended, Classified National Security Information."* Federal Register, Vol. 68. March 28, 2003. p. 15315.

77 – Shea, Dana A. "Balancing Scientific Publication and National Security Concerns: Issues for Congress." Report for Congress. Order Code RL31695. January 10, 2003: 12.

78 – http://www.usda.gov/da/ocpm.securityguideemployees/prepubl.htm

79 – Knezo, op. cit., 8.

80 – Randerson, James. New Scientist Online News. October 17, 2001. See also Altschul, Jessica. "Commercial Spy Satellites Pose a Challenge to Pentagon Planners." JINSA Jewish Institute for National Security Affairs, Feb. 28, 2002. U.S. Government controls appear to be authorized by Presidential Decision Directive 23 (PPD-23), Foreign Access To Remote Sensing Space Capabilities,

Mar. 10, 1994. See also CRS Report RL31218 *Commercial Remote Sensing by Satellite: Status and Issues*.

81 – Knezo, op. cit., 9.

82 – "Possession, Use, and Transfer of Select Agents and Toxins; Interim Final Rule." Federal Register, Vol. 240, No. 67. December 13, 2002. pp. 76885-76905.

83 – Knezo, op. cit., 9.

84 – "Rethinking Classification: Better Protection and Greater Openness." Report of the Commission on Protecting and Reducing Government Secrecy. URL: http://www.dss.mil/seclib/govsec/chap2.htm (July 28, 2003): p. 11.

85 – Foreign Affairs Manual: SBU Information. Department of State. URL: http://foia.state.gov/docs/12fam/12m0540.pdf (August 1, 2003).

86 – 12 FAM 540, Sensitive but Unclassified Information (SBU), (TL:DS-61; 10-01-1999) 12 FAM 541 SCOPE, (TL:DS-46; 05-26-1995)

87 – 12 FAM 540, Sensitive but Unclassified Information (SBU), (TL:DS-61; 10-01-1999) 12 FAM 541 SCOPE, (TL:DS-46; 05-26-1995)

88 – Deptartment of State Telegram, to All Diplomatic and Consular Posts US Office Pristina Special Embassy Program Executive Order 12958: N/a Tags: Acoa Subject: Guidance for Drafting SBU," Telegram Ref: 95 State 232445. URL: http://www.fas.org/sgp/news/2000/02/sbu.html (August 1, 2003).

89 – 12 FAM 545, Responsibilities, U.S. Department of State, Foreign Affairs Handbook, p.2 of 2

90 – Knezo, op. cit., 18.

91 – Appendix 3C, Controlled Unclassified Information," in DoD 5200.1-R, Information Security Program, Jan. 1997, issued by Assistant Secretary of Defense for Command, Control, Communications and Intelligence. URL: http://www.fas.org/irp/doddir/dod/5200-1r/appendix_c.htm (August 15, 2003).

92 – 2-202 Access to FOUO Information. URL: http://www.fas.org/irp/doddir/dod/5200-1r/appendix_c.htm (August 15, 2003).

93 – Smith, Stuart D. "Sensitive But Unclassified Data; Identification and Protection Solutions," Prepared for U.S. Army Material Command Information Assurance Program Manager. July 2002. pp. 4-5.

94 – Smith, op. cit., p.6

95 – ibid.

96 – “Glossary.”. Safeguards and Security. U.S. Department of Energy. December 18, 1995. p. 132.

97 – General Services Administration, Public Buildings Services Order 3490.1. March 8, 2002.

98 – Authorized by Title 49 U.S.C. 40119; regulations were included in Title 14 CFR Part 191.

99 – “Information Security”. NASA Security Procedures and Guidelines With Change 1, Section 4.4.7.2 of Chapter 4. September 13, 2002.

100 – Freedom of Information Act (FOIA). United States Department of Justice website. URL: http://www.usdoj.gov/04foia/ (August 25, 2003).

101 – “Fundamental Infosec Policy.” Department of the Navy Information Systems Security (INGODSRV) Program, SECNAVINST 5239.3. July 14, 1995. Source: http://www.fas/org/irp/doddir/navy/secnavinst/5239_3.htm. Also available at http://www.onr.navy.mil/sci_tech/industrial/nardic/pubs_list.asp?Letter=S

102 – Knezo, op. cit., 23.

103 – “National Policy on Technical Surveillance Countermeasures.” Issued by the Office of the Secretary, Department of Defense. Federal Register, Vol. 63, No. 20. January 30, 1998. pp. 4582-4583.

104 – Section 19.3, Scope, in section 375 DM 19, Department of the Interior, Departmental Manual, effective data: 4/15/02.

105 – White House Memorandum for the Heads of Executive Departments and Agencies From Andrew H. Card, Jr., The White House, Subject: “Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security.” March 19, 2002. URL: http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm (August 15, 2003).

106 – Memorandum for Departments and Agencies, From Laura L.S. Kimberly, Richard L. Huff, and Daniel J. Metcalfe, Information Security Oversight Office, National Archives and Records Administration [NARA], Subject: “Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Records Related to Homeland Security.” March 19, 2002. http://www.usdoj.gov/oip/foiapost/2002foiapost.htm (August 15, 2003).

107 – Ibid

108 – "New Attorney General FOIA Memorandum Issued," FOIA Post, October 15, 2001. This Department of Justice release includes "Memorandum for Heads of all Federal Departments and Agencies, From: John Ashcroft, Attorney General, Subject: The Freedom of Information Act, October 15, 2001". Available at http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm

109 – Ibid

110 – Ibid

111 – Ibid

112 – Shea, op. cit., 14-15.

113 – Department of Homeland Security Act, P.L. 107-296. November 2, 2002.

114 – Knezo, op. cit., 27.

115 – Knezo, op. cit., 28.

116 – http://www.fas.org/sgp/library.jsc/

117 – Report of the Commission on Protecting and Reducing Government Secrecy, 1997, op. cit.

118 – Chap. V. Information Age Insecurity, in Report of the Commission on Protecting and Reducing Government Secrecy, 1997, op. cit.

119 – Commission on Science and Security, John J. Hamre, chairman, Science and Security in the 21st Century: A Report to the Secretary of Energy on the Department of Energy Laboratories, Apr. 2002, Washington, D.C., Center for Strategic and International Studies, pp. 55-56

120 – Science and Security in the 21st Century, op. cit., p. 57

121 – Information Security Program, 3-27-97 and Draft DOE Glossary" from http://labs.ucop.edu/internet/security/brief00/#Anchor-SECURITY-3800

122 – Steve Aftergood and Henry Kelly, "Making Sense of Information Restrictions After September 11", FAS Public Interest Report, March/April 2002

123 – Science and Technology: Secrets and Lives; Academic Freedom," The Economist, Mar. 9, 2002

124 – Laura Gordon-Murnane, “Access to Government Information in a Post 9/11 World,” Searcher, June 1, 2002

125 – Peg Brickly, “New Antiterrorism Tenets Trouble Scientists,” The Scientist, October 28, 2002, referring to a September 19, 2002 Academy press release

126 – Martin Enserink, “Science and Security: Entering the Twilight Zone of What Material to Censor,” Science, Nov. 22, 2002, p. 1548

127 – “Presidents Statement on Science and Security in an Age of Terrorism, From Bruce Alberts, William A. Wulf, and Harvey Fineberg, Presidents of the National Academies,” October 18, 2002

128 – David Malakoff, “Researchers Urged to Self-Censor Sensitive Data,” Science, Jan. 17, 2003, p. 321

129 – Raymond A. Zilinskas and Jonathan B. Tucker, “Limiting the Contribution of the Open Scientific Literature to the Biological Weapons Threat,” Journal of Homeland Security, December 2002. See also Statement by Dr. Anthony Fauci, Director of the NIH National Institute of Allergy and Infections Diseases (NIAID) on October 3, 2002 Or Benjamin Y. Lum, “Security Exceptions to Transparency in Publishing NIH-funded Research Will Be Rare, Fauci Says,” Washington Tax, October 11, 2002

130 – Actions of the ALA Council, 2002 Annual,” June 13-19, 2002, Atlanta, GA. American Library Association. “Restrictions on Access to Government Information (RAGI) Report.” Task Force on Restrictions on Access to Government Information. June 9, 2003.

131 – http://www.fas.org/sgp/congress/2002/hres514.html

132 – For reports on the hearing, see: Anne Marine Borrego, “In Testimony, University Officials Reject ‘Sensitive’ Designation for Scientific Research,” Chronicle of Higher Education, October 11, 2002, “Impact of Homeland Security on Research and Education,” FYI, American Institute of Physics Bulletin of Science Policy News, October 18, 2002, and Cheryl Bolen, “Panel Considers Difficult Balance Between Open Research, Security,” Daily Report for Executives, October 11, 2002

133 – http://www.whitehouse.gov/news/releases/2002/11/20021125-10.html

134 – “OMB Tackles Sensitive But Unclassified Information,” Secrecy News, September 3, 2002

135 – ”Freedom of Information Act Guide and Privacy Act Overview, May 2002, edition, op. cit., p. 17, with the discussion based on Ashcroft memorandum of October 15, 2001 and White House Card Memorandum of March 19, 2002

136 – Freedom of Information Act Guide and Privacy Act Overview, May 2002, edition, op. cit., pp. 16-17, with the discussion based on Ashcroft memorandum of October 15, 2001 and White House Card Memorandum of March 19, 2002

137 – Statement of Hon. John H. Marburger, Director, Office of Science and Technology Policy Before the Committee on Science, October 10, 2002

138 – 66 Fed. Reg. 64345. December 12, 2001. 67 Fed. Reg. 61463. September 30, 2002. 67 Fed. Reg. 31109. May 9, 2002. (Respectively).

139 – Aftergood, Steven. “Making Sense of Government Information Restrictions.” Issues in Science and Technology. Summer 2002

140 – Gordon-Murnane, op. cit.

141 – Block, Marylaine. “Vanishing Act: The U.S. Government’s Disappearing Data. ExLibris. December 6, 2002.

142 – ibid.

143 – “The Bush Administration’s Secrecy Policy: A Call to Action to Protect Democratic Values.” OMB Watch. October 25, 2002.

144 – Morgan, Dan. “Disclosure Curbs in Homeland Bill Decried: Information From Companies at Issue.” Washington Post. November 16, 2002. p. A13.

145 – Morgan, op. cit.

146 – Bohn, Kevin. “ACLU files lawsuit against Patriot Act.” cnn.com. July 30, 2003. URL: http://www.cnn.com/2003/LAW/07/03/patrio.act/index.html (July 31, 2003).

147 – Graham, Mary. “The Information Wars.” The Atlantic Monthly. September 2002. pp. 36-38

148 – EPA Issues Instructions to Utilities on Submitting Threat Assessments.” Daily Report for Executives. January 8, 2003. p. A-24.

149 – “Notice of Proposed Rulemaking.” Federal Energy Regulatory Commission. Federal Register. September 13, 2002. pp. 57994-58006.

150 – Gordon-Murnane, op. cit.

151 – Rash, Wayne. “Stupidity trumps security.” InfoWorld. May 2, 2003. URL: http://www.infoworld.com/article/03/05/02/18secadvise_1.html (August 25, 2003).

REFERENCES - COMPLETE

"Remarks of J. William Leonard Director, Information Security Oversight Office (ISOO) at the National Classification Management Society's (NCMS) Annual Training Seminar Fort Worth, Texas July 16,2002." http://www.fas.org/sgp/isoo/ncms071602.html

HRES 514 IH, 107th Congress, 2d Session, "Expressing Serious Concern Regarding the Publication of Instructions on How to Create a Synthetic Human Polio Virus." Mr. Weldon of Florida. July 26,2002. http://fas.org/sgp/congress/2002/hres514.html

Moteff, John, Copeland, Claudia, and Fischer, John. "Critical Infrastructures: What Makes an Infrastructure Critical?" Report for Congress. January 29, 2003, http://www.fas.org order code RL31556

Shea, Dana A. "Critical Infrastructure: Control Systems and the Terrorist Threat." Report for Congress. February 21, 2003, http://www.fas.org order code RL31534

Knezo, Genevieve J. "'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy." Report for Congress. April 2, 2003. http://www.fas.org order code RL31845

Smith, Stuart D. "Sensitive But Unclassified Data; Identification and Protection Solutions." Prepared for U.S. Army Material Command Information Assurance Program Manager. July 2002. pp. 4-5

Shea, Dana A. "Balancing Scientific Publication and National Security Concerns: Issues for Congress." Report for Congress. January 10, 2003. http://www.fas.org order code RL31695

"Restrictions on Access to Government Information (RAGI) Report" by the American Library Association Committee on Legislation & American Library Association Government Documents Round Table, Task Force on Restrictions on Access to Government Information issued by the American Library Association. June 9, 2003

"Critical Infrastructure Protection and the Endangerment of Civil Liberties", an assessment of the President's Commission on Critical Infrastructure Protection (PCCIP). Electronic Privacy Information Center, Washington, DC. EPIC Staff, first edition 1998. http://www.epic.org/reports/epic-cip.html

"Developing a Departmental Security Plan." Introduction to Departmental Security Planning. RUSecure. August 18, 2003. http://rusecure.rutgers.edu/secplan/plan.html

Breeding, Alexander J. “Make IT Governance an Integral Part of the Enterprise”. June 16, 2003. CNET Networks. http://techrepublic.com.com/5100-6298-5035046.html?tag=search

Olsen, Geir. “Create a Plan for Security Preparedness.” Learn how to establish a solid security plan and take advantage of new features in .NET to protect your organization. December 2002. http://www.fawcette.com/dotnetmag/2002_12/magazine/columns/security

Loos, Mark. “Implementing a Local Security Program to Protect National Infrastructure System Companies and Facilities.” April 8, 2002. SANS Paper. URL: http://www.sans.org/rr/paper.php?id=822 .

Lawson, Shannon M. “Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure.” February 19, 2002. SANS Paper, http://rr.sans.org/infowar/us_critical.php

“Understanding SCADA System Security Vulnerabilities.” RIPTECH. January 2001. http://www.riptech.com/pdfs/power_whitepaper_scada.pdf

Verton, Dan. “Utility Companies Face Barrage of Cyberattacks.” January 21, 2002. Computerworld. http://www.computerworld.com/itresources/rcstory/0,4167,sto67581_key73,00.html

Verton, Dan. “Web Sites Seen as Terrorist Aids.” February 11, 2002. Computerworld. http://www.computerworld.com/cwi/stories/0,1199,nav47-81_sto68181,00.html

Burkhart, Lori A. “The Cybercrime Threat.” December 2001. puc.com. http://www.pur.com/cybercrime%20threat.html

Thibodeau, Patrick. “Official: Terrorists Used Internet to Get Info on Potential Targets.” February 13, 2002. Computerworld. http://www.computerworld.com/storyba/0,4125,nav47_sto68281,00.html

“Dubious Secrets.” National Security Archive Electronic Briefing Book No. 90. Edited by Jeffrey Richelson, William Burr and Thomas Blanton (with contributions from Michael Evans and Robert Wampler). May 21, 2003. http://www.gwu.edu/~nsarchiv/nsaebb/nsaebb90/index2.htm

“Memorandum for Department of Energy FOIA Officers.” Abel Lopez, Director, FOIA and Pay Division. March 21, 2002. Subj: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security.

"Executive Order 13292" Further Amendment to Executive Order 12958, as Amended, Classified National Security Information. The White House. Office of the Press Secretary. March 25, 2003. http://www.fas.org/sgp/bush/eoamend.html

McGeary, Johanna. "An Invitation to Terrorists?" This time, officials say, it wasn't terrorism. But what about the next? Time Online Edition. August 25, 2003. http://www.time.com/time/magazine/article/9,9171,1101030825-46273,00.html

Blumenfeld, Laura. "Dissertation Could Be Security Threat." Student's Maps Illustrate Concerns About Public Information. Washington Post. July 8, 2003. http://www.washingtonpost.com/ac2/wp-dyn/a23689-2003Jul7?language=printer

"Plant Safety: Defense in Depth." Nuclear Energy Institute. http://www.nei.org/index.asp?catnum=2&catid=55

"Foreign Information Warfare Programs and Capabilities." John M. Deutch, Director of Central Intelligence. 25 June 1996. http://www.cia.gov/cia/public_affairs/speeches/1996/dci_testimony_0625996.html

"Protecting National Security Under the FOIA." FOIA Update, Vol. VI, No.1. Winter 1985. http://www.usdoj.gov/oip/foia_updates/Vol_VI_1/page1.htm

Moteff, John D. "Critical Infrastructures: Background, Policy, and Implementation." Report for Congress. February 10, 2003. http://www.fas.org order code RL30153

Moteff, John D. "Critical Infrastructure Information Disclosure and Homeland Security." Report for Congress. January 29, 2003. and Gina Marie Stevens. http://www.fas.org order code 31547

Matthews, William. "Sensitive Label Strikes Nerve." October 31, 2002. http://www.fcw.com/fcw/articles/2002/1028/web-info-10-31-02.asp

Graham, Mary. "The Information Wars." The Atlantic Monthly. September 2002. http://www.theatlantic.com/issues/2002/09/graham.htm

"Chronology of Disappearing Government Information." Data collected through October 31, 2002. Compiled by Barbara Miller for ALA/GODORT Education Committee with special assistance of Karrie Peterson. http://tigger.uic.edu/~tfontno/chr.html

"Federal Judges, Agencies Block Online Access to Public Records." Associated Press. October 12, 2001. http://www.freedomforum.org/templates/document.asp?documentID=15143

"White House Puts New Controls on Federal Web Sites." Associated Press. March 22, 2002. http://www.freedomforum.org/templates/document.asp?documentID=15933

"Web Sites Remove Data, Citing Security Concerns in Wake of Attacks." Associated Press. October 04, 2001. http://www.freedomforum.org/templates/document.asp?documentID=15066

"Fact Sheet" Department of Homeland Security, Procedures for Handling Critical Infrastructure Information; Proposed Rule – published in 68 Fed. Reg. 18525; What the Rule Does Not Do: No Workable Procedures for Review of Industry CII Claims. Rena Steinzor. http://www.progressiveregulation.org

Koprowski, Gene J. "Hacking the Power Grid." Wired News. June 4, 1998. http://wired.com/news/print/0,1294,12746,00.html

Borland, Jerry. "WTC Disaster Causes Extensive Damage to Electric Infrastructure." PowerQuality. September 14, 2001. http://www.powerquality.com/newsarticle.asp?mode=print&newsarticleid=231243&releaseid=&srid=10215&magazineid=28/1/2003

Poulsen, Kevin. "Slammer Worm Crashed Ohio Nuke Plant Network." SecurityFocus. August 19, 2003. http://www.securityfocus.com/news/6767

Verton, Dan. "U.S. Infrastructure Shaken by Terrorist Attack." September 11, 2001. Computerworld. http://www.computerworld.comsecuritytopics/security/story/0,10801,63719,00.html

"Report of the Commission on Protecting and Reducing Government Secrecy." Rethinking Classification: Better Protection and Greater Openness. November 14, 2001. http://www.dss.mil/seclib/govsec/chap2.htm

"Cyber Security of the Electric Power Industry." December 2002. Institute for Security Technology Studies at Dartmouth College. http://www.ists.dartmouth.edu/ISTS/ists_docs/cselectric.pdf

Bourge, Christian. "Farms Vulnerable to Terrorism, Study Says." September 14, 2002. United Press International. http://www.upi/com/print.cfm?StoryID=20020913-061851-6670r

"New England's Bulk Electric Power Grid Operating Procedures and Guidelines." May 2003. http://www.iso-ne.com/iso_news/Information_Kit/02_Power_Grid_Operating_Procedures_and_Guidelines.pdf

Friend, Tim. “Power Grid Vulnerable to Attack, Report Warns.” USA Today. June 24, 2002. http://www.usatoday.com/news/nation/2002/06/24/power.htm

Weisman, Robyn. “California Power Grid Hack Underscores Threat to U.S.” NewsFactor Network. June 13, 2001. http://www.newsfactor.com/perl/printer/11220/

Kelly, Russ. “Electric Power Grid Failures Likely.” June 1998. http://www.russkelly.com/rkelect.html

Malveaux, Suzanne. “Bush: Blackout is ‘Wake-Up’ Call.” cnn.com. August 15, 2003. http://www.cnn.com/2003/allpolitics/08/15/bush.blackout/index.html

“Planes, Trains Recovering from Blackout.” Associated Press. cnn.com. August 15, 2003. http://www.cnn.com/2003/travel/08/15/air.traffic.ap/index.html

Botelho, Greg. “Lights Returning in Power Grid-Lock.” August 15, 2003. cnn.com. http://www.fox11az.com/news/other/stories/kmsb_local_power_081503.b6a7206.html

Kehnemui, Sharon. “Massive Blackout Cripples Northeast.” August 14, 2003. Foxnews.com. http://www.foxnews.com/printer_friendly_story/0,3566,94772,00.html

“Power Industry Has ‘No Unified Plan’ to Improve Security at Plants.” platts.com. http://www.platts.com/features/ussecurity/power.shtml

“Computer Virus Hinders Air Canada Operations.” Associated Press. August 19, 2003. http://www.securityfocus.com/news/6770

“Computer Virus Strikes CSX Transportation Computer.” csx.com. August 20, 2003. http://www.csx.com/?fuseaction=company.news_detail&l=45722&news_year=-1

Sandler, Todd. “An Economic Perspective on Transnational Terrorism.” School of International Relations, University of Southern California, and Walter Enders, Department of Economics, Finance, and Legal Studies, University of Alabama. February 2002. http://www.ecaar.org/articles/sandlerDIW.pdf

DeYoung, Timothy J., and Sperling, Modrall. “Coordinating Efforts to Secure American Public Water Supplies.” March 11, 2002. http://www.modrall.com/articles/article_98.html

Rappaport, Edward. “Terrorism: The New Occupational Hazard.” Analyst in Industry Economics, Domestic Social Policy Division. March 29, 2002. http://www.fas.org order code RL31387

Chalk, Peter. “Replace the Weak Links in the Food Chain.” RAND Policy Analyst. August 2002. RAND.
http://www.rand.org/publications/randreview/issues/rr.08.02/foodchain.html

Messmer, Ellen. “Hackers Set Up Shop in State Agency’s Server.” Network World. August 4, 2003. p. 60

“Man Jailed for Linking to Bomb Sites.” Associated Press. August 5, 2003. cnn.com.
http://www.cnn.com/2003/tech/internet/08/05/anarchist.prison.ap/index.html

Dizard III, Wilson P. “Judge Orders Interior to Shut Off Internet Connections.” Government Computer News. gcn.com.
http://www.gcn.com/vol1_no1/security/22935-1.html

Stidham, Jonathan. “Can Hackers Turn Your Lights Off?” The Vulnerability of the US Power Grid to Electronic Attack. September 26, 2001.
http://www.sans.org/rr/hackers/lights.php

“Heritage Foundation Report on Infrastructure Protection.” Heritage Foundation. January 8, 2002.
http://www.itsa.org/itsnews.nsf/0/752ad9b60686c4a085256b3d004163d?opendocument

Ackerman, Robert K. “Hidden Hazards Menace U.S. Information Infrastructure.” August 1999. Signal Magazine 1999.
http://us.net/signal/archive/august99/hidden-aug.html

Tiemann, Mary. “Safe Drinking Water Act: State Revolving Fund Program.” Specialist in Environmental Policy, Resources, Science, and Industry Division. Report for Congress. January 10, 2002. http://www.fas.org order code 97-677 ENR

“Critical Infrastructure Information Security Act of 2001.” September 24, 2001.
http://bennett.senate.gov/s1456.html

“Sensitive But Unclassified Provisions in the Homeland Security Act of 2002.” June 11, 2003. OMB Watch.
http://www.cdt.org/security/usapatrior/030611omb.pdf

“Critical Infrastructure Protection in the Modern World.” SIPAC. Remarks of Texas Attorney General John Cornyn. November 27, 2001.
http://www.oag.state.tx.us/sipac/sipac_modern.htm

"1 Dead, 3 Wounded in Shooting at U.S. Capitol." Associated Press. July 24, 1998. cnn.com. http://www.cnn.com/US/9807/24/dc.shooting.02/

Mussington, David, and Don, Bruce. "Protecting Critical Infrastructure." RAND. http://www.rand.org/publications/randreview/issues/rr.08.02/infrastructure.html

Higgins, Mike. "The Internet: Business Blessing or Terrorist's Tool?" December 2001. SC Magazine. http://www.scmagazine.com/scmagazine/2001_12/cover/cover.html

"Intelligence Organizations – United States" http://www.sfu.ca/igs/casis/links/intel_orgs_us.html

Rash, Wayne. "Stupidity Trumps Security." InfoWorld. May 2, 2003. http://www.infoworld.com/article/03/05/02/18secadvise_1.html

"Map", showing main power grids across the United States. August 15, 2003. http://www.cnn.com/interactive/us/0308/blackout/content.1.html

"Nuclear Waste Transportation Routes." Highway and rail routes most likely to be used to transport high-level nuclear waste to Yucca Mountain, Nevada. January 1995. http://www.state.nv.us/nucwaste/states/us.htm

"California Energy Maps." Map of Power Plants in California. June 26, 2003. http://www.energy.ca.gov/maps/power_plant.html

"California Energy Maps." California's Major Electric Transmission Lines. September 6, 2000. http://www.energy.ca.gov/maps/transmission_lines.html

Appendix A

All information appearing in this appendix has been gleaned from "'Sensitive But Unclassified' and Other Federal Security Controls on Scientific and Technical Information: History and Current Controversy." Report for Congress. Order Code RL31845. April 2, 2003. Genevieve J. Knezo, Specialist, Science and Technology Policy, Resources, Science, and Industry Division.

The earliest references to sensitive but unclassified information appeared in 1977.

Telecommunications Protection Policy (PD/NSC-24). This presidential directive on Telecommunications Protection Policy dictated that information must be protected that was unclassified but sensitive "that could be useful to an adversary". No further definition was provided.

National Security Decision Directive 145 (NSDD-145). This directive was issued in 1984 and provided that "sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest …" should be "protected in proportion to the threat of exploitation and the associated potential damage to the national security." The term "sensitive, but unclassified" was not defined. This directive did mention that even unclassified information could "reveal highly classified and other sensitive information" harmful to the national security if it was compiled properly. Except for responsibilities provided by Presidential Directive 24 (Carter, 1977), NSDD-145 was rescinded by National Security Directive 42 (National Policy for the Security of National Security Telecommunications and Information Systems) July 5, 1990. The GAO had called for "clearly defined" types of information considered to be sensitive but unclassified in congressional testimony in 1985 (GAO/OSI-94-2, p. 15).

National Policy on Protection of Sensitive, but Unclassified Information in Federal Government Telecommunications and Automated Information Systems, NTISSP No. 2. This document was issued by John Poindexter, President Reagan's National Security Advisor, in October of 1986. In it, he advocated the widening of protection of "sensitive, but unclassified" information for reasons of national security.

"Sensitive, but unclassified information is information that disclosure, loss, misuse, alteration or destruction of which could adversely affect national security or other Federal Government interests. National security interests are those unclassified matters that relate to the national defense or the foreign relations of the U.S. government. Other government interests are those related, but not limited to the wide range of government or government-derived economic, human, financial, industrial, agriculture, technological, and law enforcement

information, as well as the privacy or confidentiality of personal of commercial proprietary information provided to the U.S. Government by its citizens."

Debate over this document centered on the control of the government over civilian information activities. The document was withdrawn in 1987 following passage of the Computer Security Act of 1987.

The Computer Security Act of 1987 (P.L. 100-235). This act passed by Congress has been codified at 40 USC 1441. In it, they state "improving the security and privacy of sensitive information in Federal computer systems is in the public interest, and hereby creates a means for establishing minimum acceptable security practices for such systems, without limiting the scope of security measures already planned or in use". It also called for the creation of a computer standards program within the National Institute of Standards and Technology (NIST [previously known as the National Bureau of Standards]).

Additionally, this law defined "sensitive" as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy".

Note that this limits the designation of sensitive to information that is not classified. Each agency was responsible for determining what information should be designated for official use or released. Because this act referred to "sensitive" information that is not classified, some say this is the first reference (and effective definition) of sensitive but unclassified.

National Institute of Standards and Technology (NIST) Guidelines. In 1992, NIST issued guidelines regarding protecting sensitive information pursuant to the Computer Security Act of 1987. They stated:

"Interpretation of the Computer Security Act's definition of sensitive is, ultimately, an agency responsibility. Typically, protecting sensitive information means providing for one or more of the following: Confidentiality: disclosure of the information must be restricted to designated parties; Integrity: the information must be protected from errors or unauthorized modification; Availability: the information must be available within some given time frame" (CSL Bulletin: "Advising Users on Computer System Technology," Nov. 1992, http://nsi.org/library/compsec/sensitiv.txt).

NIST urged agency owners to "use a risk-based approach to determine" potential harm of inadequately protected information. They further emphasized "information 'owners', not system operators, should determine what protection

their information requires. The type and amount of protection needed depends on the nature of the information and the environment in which it is processed. The controls to be used will depend on the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in the system" (CSL Bulletin: "Advising Users on Computer System Technology," Nov. 1992).

Freedom of Information Act. The Freedom of Information Act (FOIA) was passed in 1966. It was enacted to ensure public access to certain information held by government agencies. FOIA provides the following exceptions:

(1) information classified in the interest of national defense or foreign policy,
(2) internal personnel rules and practices of an agency,
(3) information specifically exempted from disclosure by statute.
(4) Trade secrets and commercial or financial information obtained from a person and privileged or confidential
(5) Inter-agency or intra-agency memoranda or letters reflecting predecisional attitudes
(6) Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy
(7) Specified types of law enforcement records or information
(8) Financial institution regulation or supervision reports, and
(9) Geological and geophysical information and data concerning wells

As previously mentioned, the Computer Security Act delineated 3 reasons to consider non-classified information as sensitive: adverse effects on the national interest, adverse effects on the conduct of federal programs, and privacy. It did specifically state it was not authority to withhold information requested under FOIA. This was reiterated by NIST guidelines as stated in 1992. Note that these acts do not state that information exempt from FOIA production is to be considered "sensitive" necessarily. Likewise, simply because information has been designated sensitive does not mean it is exempt from FOIA production.

Appendix B

The following information copied directly from the United States Department of Justice, Office of Information and Privacy, FOIA Post website, located at: http://www.usdoj.gov/oip/foiapost/2002foiapost10.htm (August 25, 2003).

Guidance on Homeland Security Information Issued

The following memorandum regarding the safeguarding and protection of sensitive homeland security information was issued to the heads of all federal departments and agencies by the White House Chief of Staff on March 19. It forwards a memorandum from the Information Security Oversight Office and the Office of Information and Privacy, also set out below, which provides additional guidance on this important subject.

* * * * *

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: ANDREW H. CARD, JR.
Assistant to the President and Chief of Staff

SUBJECT: Action to Safeguard Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security

As noted in many discussions during the past several months, you and your department or agency have an obligation to safeguard Government records regarding weapons of mass destruction. Weapons of mass destruction include chemical, biological, radiological, and nuclear weapons. 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 the current locations of stockpiles of nuclear materials that could be exploited for use in such weapons, should not be disclosed inappropriately.

I asked the Acting Director of the Information Security Oversight Office and the Co-Directors of the Justice Department's Office of Information and Privacy to prepare guidance for reviewing Government information in your department or agency regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation and the safety of our people. Their guidance is attached, and it should be distributed to appropriate officials within your department or agency, together with this memorandum, to assist in your undertaking an immediate reexamination of current measures for identifying and safeguarding all such information at your department or agency.

All departments and agencies should review their records management procedures and, where appropriate, their holdings of documents to ensure that they are acting in accordance with the attached guidance. They

should report the completion, or status, of their review to this office through the Office of Homeland Security no later than 90 days from the date of this memorandum.

If agency officials need assistance in determining the classification status of records related to the development or use of weapons of mass destruction, they should contact the Information Security Oversight Office, at 202-219-5250. For assistance in determining the classification of nuclear and radiological weapons classified under the Atomic Energy Act, they should contact the Department of Energy's Office of Security, at 202-586-3345. If they need assistance in applying exemptions of the Freedom of Information Act (FOIA) to sensitive but unclassified information, they should contact the Justice Department's Office of Information and Privacy (OIP), at 202-514-3642, or consult OIP's FOIA Web site at www.usdoj.gov/04foia/index/html.

* * * * *

MEMORANDUM FOR DEPARTMENTS AND AGENCIES

FROM: LAURA L.S. KIMBERLY
Acting Director
Information Security Oversight Office

RICHARD L. HUFF
DANIEL J. METCALFE
Co-Directors
Office of Information and Privacy
Department of Justice

SUBJECT: Safeguarding Information Regarding Weapons of Mass Destruction
and Other Sensitive Records Related to Homeland Security

At the request of the Assistant to the President and Chief of Staff, we have prepared this memorandum to provide guidance for reviewing Government information regarding weapons of mass destruction, as well as other information that could be misused to harm the security of our nation or threaten public safety. It is appropriate that all federal departments and agencies consider the need to safeguard such information on an ongoing basis and also upon receipt of any request for records containing such information that is made under the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). Consistent with existing law and policy, the appropriate steps for safeguarding such information will vary according to the sensitivity of the information involved and whether the information currently is classified.

I. Classified Information

• If the information currently is classified and is equal to or less than 25 years old, it should remain classified in accordance with Executive Order 12958, Sec. 1.5 and Sec. 1.6. Although classified information generally must be declassified within 10 years of its original classification, classification or reclassification may be extended for up to 25 years in the case of information that could reasonably be expected to "reveal information that would assist in the development or use of weapons of mass destruction." Id., Sec. 1.6(d)(2).

• If the information is more than 25 years old and is still classified, it should remain classified in accordance with Executive Order 12958, Sec. 3.4(b)(2), which authorizes agency heads to exempt from automatic declassification any "specific information, the release of which should be expected to . . . reveal information that would assist in the development or use of weapons of mass destruction." (Agencies should note that the automatic declassification date for any classified information over 25 years old that involves the equities of more than one agency was extended until April 2003 by Executive Order 13142. Agencies have until then to exempt such information from automatic declassification under any one of the pertinent exemption categories in Executive Order 12958, Sec. 3.4(b).)

In this regard, agencies should note that Department of Defense (DOD) information that involves the equities of more than one DOD component is considered to have multi-agency equities. Information maintained by the Defense Technical Information Center (DTIC) or the National Archives and Records Administration (NARA) also is deemed to have multi-agency equities, i.e., those pertaining to DTIC or NARA and those pertaining to the component agency or agencies that created the information.

II. Previously Unclassified or Declassified Information

• If the information, regardless of age, never was classified and never was disclosed to the public under proper authority, but it could reasonably be expected to assist in the development or use of weapons of mass destruction, it should be classified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8(d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).

• If such sensitive information, regardless of age, was classified and subsequently was declassified, but it never was disclosed to the public under proper authority, it should be reclassified in accordance with Executive Order 12958, Part 1, subject to the provisions of Sec. 1.8(d) if the information has been the subject of an access demand (or Sec 6.1(a) if the information concerns nuclear or radiological weapons).

III. Sensitive But Unclassified Information

In addition to information that could reasonably be expected to assist in the development or use of weapons of mass destruction, which should be classified or reclassified as described in Parts I and II above, departments and agencies maintain and control sensitive 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 need to protect such sensitive information from inappropriate disclosure should be carefully considered, on a case-by-case basis, together with the benefits that result from the open and efficient exchange of scientific, technical, and like information.

All departments and agencies should ensure that in taking necessary and appropriate actions to safeguard sensitive but unclassified information related to America's homeland security, they process any Freedom of Information Act request for records containing such information in accordance with the Attorney General's FOIA Memorandum of October 12, 2001, by giving full and careful consideration to all applicable FOIA exemptions. See *FOIA Post*, "New Attorney General FOIA Memorandum Issued" (posted 10/15/01) (found at www.usdoj.gov/oip/foiapost/2001foiapost19.htm), which discusses and provides electronic links to further guidance on the authority available under Exemption 2 of the FOIA, 5 U.S.C. § 552(b)(2), for the protection of sensitive critical infrastructure information. In the case of information that is voluntarily submitted to the Government from the private sector, such information may readily fall within the protection of Exemption 4 of the FOIA, 5 U.S.C. § 552(b)(4).

As the accompanying memorandum from the Assistant to the President and Chief of Staff indicates, federal departments and agencies should not hesitate to consult with the Office of Information and Privacy, either with general anticipatory questions or on a case-by-case basis as particular matters arise, regarding any FOIA-related homeland security issue. Likewise, they should consult with the Information Security Oversight Office on any matter pertaining to the classification, declassification, or reclassification of information regarding the development or use of weapons of mass destruction, or with the Department of Energy's Office of Security if the information concerns nuclear or radiological weapons.

* * * * *

These memoranda are being made available through the Office of Information and Privacy's main FOIA Web site, as well as through *FOIA Post*, to encourage all agency FOIA personnel to be particularly aware of the careful attention that should be paid to any FOIA request that encompasses homeland security-related information. *(posted 3/21/02)*

Appendix C

The following information has been copied directly from the United States Department of Justice website, at the following location: http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm

The Freedom of Information Act 5 U.S.C. § 552, As Amended By Public Law No. 104-231, 110 Stat. 3048

Below is the full text of the Freedom of Information Act in a form showing all amendments to the statute made by the "Electronic Freedom of Information Act Amendments of 1996." All newly enacted provisions are in boldface type.

§ 552. Public information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public--

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the methods whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedure, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph, matter reasonably available to the class of persons affected

thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

> (2) Each agency, in accordance with published rules, shall make available for public inspection and copying--
>
> > (A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;
> >
> > (B) those statements of policy and interpretations which have been adopted by the agency and are not published in the Federal Register; ~~and~~
> >
> > (C) administrative staff manuals and instructions to staff that affect a member of the public;
> >
> > **(D) copies of all records, regardless of form or format, which have been released to any person under paragraph (3) and which, because of the nature of their subject matter, the agency determines have become or are likely to become the subject of subsequent requests for substantially the same records; and**
> >
> > **(E) a general index of the records referred to under subparagraph (D);**

unless the materials are promptly published and copies offered for sale. **For records created on or after November 1, 1996, within one year after such date, each agency shall make such records available, including by computer telecommunications or, if computer telecommunications means have not been established by the agency, by other electronic means.** To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, ~~or staff manual or instruction,~~ **staff manual, instruction, or copies of records referred to in subparagraph (D)**. However, in each case the justification for the deletion shall be explained fully in writing**, and the extent of such deletion shall be indicated on the portion of the record which is made available or published, unless including that indication would harm an interest protected by the exemption in subsection (b) under which the deletion is made. If technically feasible, the extent of the deletion shall be indicated at the place in the record where the deletion was made.** Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly publish, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplements thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of an index on request at a cost not to exceed the direct cost of duplication. **Each agency shall make the index referred to in**

subparagraph (E) available by computer telecommunications by December 31, 1999. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if--

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3)**(A)** Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon request for records which ~~(A)~~ **(i)** reasonably describes such records and ~~(B)~~ **(ii)** is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(B) In making any record available to a person under this paragraph, an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

(C) In responding under this paragraph to a request for records, an agency shall make reasonable efforts to search for the records in electronic form or format, except when such efforts would significantly interfere with the operation of the agency's automated information system.

(D) For purposes of this paragraph, the term "search" means to review, manually or by automated means, agency records for the purpose of locating those records which are responsive to a request.

(4)(A)(i) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying the schedule of fees applicable to the processing of requests under this section and establishing procedures and guidelines for determining when such fees should be waived or reduced. Such schedule shall conform to the guidelines which shall be promulgated, pursuant to notice and receipt of public comment, by the Director of the Office of Management and Budget and which shall provide for a uniform schedule of fees for all agencies.

(ii) Such agency regulations shall provide that--

(I) fees shall be limited to reasonable standard charges for document search, duplication, and review, when records are requested for commercial use;

(II) fees shall be limited to reasonable standard charges for document duplication when records are not sought for commercial use and the request is made by an educational or noncommercial scientific institution, whose purpose is scholarly or scientific research; or a representative of the news media; and

(III) for any request not described in (I) or (II), fees shall be limited to reasonable standard charges for document search and duplication.

(iii) Documents shall be furnished without any charge or at a charge reduced below the fees established under clause (ii) if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester.

(iv) Fee schedules shall provide for the recovery of only the direct costs of search, duplication, or review. Review costs shall include only the direct costs incurred during the initial examination of a document for the purposes of determining whether the documents must be disclosed under this section and for the purposes of withholding

any portions exempt from disclosure under this section. Review costs may not include any costs incurred in resolving issues of law or policy that may be raised in the course of processing a request under this section. No fee may be charged by any agency under this section--

(I) if the costs of routine collection and processing of the fee are likely to equal or exceed the amount of the fee; or

(II) for any request described in clause (ii)(II) or (III) of this subparagraph for the first two hours of search time or for the first one hundred pages of duplication.

(v) No agency may require advance payment of any fee unless the requester has previously failed to pay fees in a timely fashion, or the agency has determined that the fee will exceed $250.

(vi) Nothing in this subparagraph shall supersede fees chargeable under a statute specifically providing for setting the level of fees for particular types of records.

(vii) In any action by a requester regarding the waiver of fees under this section, the court shall determine the matter de novo, provided that the court's review of the matter shall be limited to the record before the agency.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine

whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. **In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).**

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under this subsection within thirty days after service upon the defendant of the pleading in which such complaint is made, unless the court otherwise directs for good cause shown.

[~~(D) Except as to cases the court considers of greater importance, proceedings before the district court, as authorized by this subsection, and appeals therefrom, take precedence on the docket over all cases and shall be assigned for hearing and trial or for argument at the earliest practicable date and expedited in every way.~~ Repealed by Pub. L. 98-620, Title IV, 402(2), Nov. 8, 1984, 98 Stat. 3335, 3357.]

(E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding. The Special Counsel, after investigation and consideration of the evidence submitted, shall submit his findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his

representative. The administrative authority shall take the corrective action that the Special Counsel recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one member shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1), (2), or (3) of this subsection, shall--

(i) determine within ~~ten days~~ **twenty days** (excepting Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency any adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

~~(B) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days. As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular request--~~

~~(i) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;~~

~~(ii) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or~~

~~(iii) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.~~

(B)(i) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the unusual circumstances for such extension and the date on which a determination is expected to be dispatched. No such notice shall specify a date that would result in an extension for more than ten working days, except as provided in clause (ii) of this subparagraph.

(ii) With respect to a request for which a written notice under clause (i) extends the time limits prescribed under clause (i) of subparagraph (A), the agency shall notify the person making the request if the request cannot be processed within the time limit specified in that clause and shall provide the person an opportunity to limit the scope of the request so that it may be processed within that time limit or an opportunity to arrange with the agency an alternative time frame for processing the request or a modified request. Refusal by the person to reasonably modify the request or arrange such an alternative time frame shall be considered as a factor in determining whether exceptional circumstances exist for purposes of subparagraph (C).

(iii) As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular requests--

> **(I) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;**
>
> **(II) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or**
>
> **(III) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject matter interest therein.**

(iv) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for the aggregation of certain requests by the same requestor, or by a group of requestors acting in concert, if the agency reasonably believes that such requests actually constitute a single request, which would otherwise satisfy the unusual circumstances specified in this subparagraph, and the requests involve clearly related matters. Multiple requests involving unrelated matters shall not be aggregated.

(C)**(i)** Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails to comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency additional time to complete its review of the records. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(ii) For purposes of this subparagraph, the term "exceptional circumstances" does not include a delay that results from a predictable agency workload of requests under this section, unless the agency demonstrates reasonable progress in reducing its backlog of pending requests.

(iii) Refusal by a person to reasonably modify the scope of a request or arrange an alternative time frame for processing the request (or a modified request) under clause (ii) after being given an opportunity to do so by the agency to whom the person made the request shall be considered as a factor in determining whether exceptional circumstances exist for purposes of this subparagraph.

(D)(i) Each agency may promulgate regulations, pursuant to notice and receipt of public comment, providing for multitrack processing of requests for records based on the amount of work or time (or both) involved in processing requests.

(ii) Regulations under this subparagraph may provide a person making a request that does not qualify for the fastest multitrack processing an opportunity to limit the scope of the request in order to qualify for faster processing.

(iii) This subparagraph shall not be considered to affect the requirement under subparagraph (C) to exercise due diligence.

(E)(i) Each agency shall promulgate regulations, pursuant to notice and receipt of public comment, providing for expedited processing of requests for records--

(I) in cases in which the person requesting the records demonstrates a compelling need; and

(II) in other cases determined by the agency.

(ii) Notwithstanding clause (i), regulations under this subparagraph must ensure--

(I) that a determination of whether to provide expedited processing shall be made, and notice of the determination shall be provided to the person making the request, within 10 days after the date of the request; and

(II) expeditious consideration of administrative appeals of such determinations of whether to provide expedited processing.

(iii) An agency shall process as soon as practicable any request for records to which the agency has granted expedited processing under this subparagraph. Agency action to deny or affirm denial of a request for expedited processing pursuant to this subparagraph, and failure by an agency to respond in a timely manner to such a request shall be subject to judicial review under

paragraph (4), except that the judicial review shall be based on the record before the agency at the time of the determination.

(iv) A district court of the United States shall not have jurisdiction to review an agency denial of expedited processing of a request for records after the agency has provided a complete response to the request.

(v) For purposes of this subparagraph, the term "compelling need" means--

(I) that a failure to obtain requested records on an expedited basis under this paragraph could reasonably be expected to pose an imminent threat to the life or physical safety of an individual; or

(II) with respect to a request made by a person primarily engaged in disseminating information, urgency to inform the public concerning actual or alleged Federal Government activity.

(vi) A demonstration of a compelling need by a person making a request for expedited processing shall be made by a statement certified by such person to be true and correct to the best of such person's knowledge and belief.

(F) In denying a request for records, in whole or in part, an agency shall make a reasonable effort to estimate the volume of any requested matter the provision of which is denied, and shall provide any such estimate to the person making the request, unless providing such estimate would harm an interest protected by the exemption in subsection (b) pursuant to which the denial is made.

(b) This section does not apply to matters that are--

(1)(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;

(2) related solely to the internal personnel rules and practices of an agency;

(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(9) geological and geophysical information and data, including maps, concerning wells.

Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection. **The amount of information deleted shall be indicated on the released portion of the record, unless including that indication would harm an interest protected by the exemption in this subsection under which the deletion is made. If technically feasible, the amount of the information deleted shall be indicated at the place in the record where such deletion is made.**

(c)(1) Whenever a request is made which involves access to records described in subsection (b)(7)(A) and--

(A) the investigation or proceeding involves a possible violation of criminal law; and

(B) there is reason to believe that (i) the subject of the investigation or proceeding is not aware of its pendency, and (ii) disclosure of the existence of the records could reasonably be expected to interfere with enforcement proceedings, the agency may, during only such time as that circumstance continues, treat the records as not subject to the requirements of this section.

(2) Whenever informant records maintained by a criminal law enforcement agency under an informant's name or personal identifier are requested by a third party according to the informant's name or personal identifier, the agency may treat the records as not subject to the requirements of this section unless the informant's status as an informant has been officially confirmed.

(3) Whenever a request is made which involves access to records maintained by the Federal Bureau of Investigation pertaining to foreign intelligence or counterintelligence, or international terrorism, and the existence of the records is classified information as provided in subsection (b)(1), the Bureau may, as long as the existence of the records remains classified information, treat the records as not subject to the requirements of this section.

(d) This section does not authorize the withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

~~(e) On or before March 1 of each calendar year, each agency shall submit a report covering the preceding calendar year to the Speaker of the House of Representatives and President of the Senate for referral to the appropriate committees of the Congress. The report shall include--~~

~~(1) the number of determinations made by such agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;~~

~~(2) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information;~~

~~(3) the names and titles or positions of each person responsible for the denial of records requested under this section, and the number of instances of participation for each;~~

~~(4) the results of each proceeding conducted pursuant to subsection (a)(4)(F), including a report of the disciplinary action taken against the officer or employee who was primarily responsible for improperly withholding records or an explanation of why disciplinary action was not taken;~~

~~(5) a copy of every rule made by such agency regarding this section;~~

~~(6) a copy of the fee schedule and the total amount of fees collected by the agency for making records available under this section; and~~

~~(7) such other information as indicates efforts to administer fully this section.~~

~~The Attorney General shall submit an annual report on or before March 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subsections (a)(4)(E), (F), and (G). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.~~

(e)(1) On or before February 1 of each year, each agency shall submit to the Attorney General of the United States a report which shall cover the preceding fiscal year and which shall include--

(A) the number of determinations made by the agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each such determination;

(B)(i) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information; and

(ii) a complete list of all statutes that the agency relies upon to authorize the

agency to withhold information under subsection (b)(3), a description of whether a court has upheld the decision of the agency to withhold information under each such statute, and a concise description of the scope of any information withheld;

(C) the number of requests for records pending before the agency as of September 30 of the preceding year, and the median number of days that such requests had been pending before the agency as of that date;

(D) the number of requests for records received by the agency and the number of requests which the agency processed;

(E) the median number of days taken by the agency to process different types of requests;

(F) the total amount of fees collected by the agency for processing requests; and

(G) the number of full-time staff of the agency devoted to processing requests for records under this section, and the total amount expended by the agency for processing such requests.

(2) Each agency shall make each such report available to the public including by computer telecommunications, or if computer telecommunications means have not been established by the agency, by other electronic means.

(3) The Attorney General of the United States shall make each report which has been made available by electronic means available at a single electronic access point. The Attorney General of the United States shall notify the Chairman and ranking minority member of the Committee on Government Reform and Oversight of the House of Representatives and the Chairman and ranking minority member of the Committees on Governmental Affairs and the Judiciary of the Senate, no later than April 1 of the year in which each such report is issued, that such reports are available by electronic means.

(4) The Attorney General of the United States, in consultation with the Director of the Office of Management and Budget, shall develop reporting and performance guidelines in connection with reports required by this subsection by October 1, 1997, and may establish additional requirements for such reports as the Attorney General determines may be useful.

(5) The Attorney General of the United States shall submit an annual report on or before April 1 of each calendar year which shall include for the prior calendar year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subparagraphs (E), (F), and (G) of subsection (a)(4). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

~~(f) For purposes of this section, the term "agency" as defined in section 551(1) of this title includes any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.~~

(f) For purposes of this section, the term--

(1) "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(2) "record" and any other term used in this section in reference to information includes any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format.

(g) The head of each agency shall prepare and make publicly available upon request, reference material or a guide for requesting records or information from the agency, subject to the exemptions in subsection (b), including--

(1) an index of all major information systems of the agency;

(2) a description of major information and record locator systems maintained by the agency; and

(3) a handbook for obtaining various types and categories of public information from the agency pursuant to chapter 35 of title 44, and under this section.

*** * * * ***

Section 12. Effective Date [not to be codified].

(a) Except as provided in subsection (b), this Act shall take effect 180 days after the date of the enactment of this Act [March 31, 1997].

(b) Sections 7 and 8 shall take effect one year after the date of the enactment of this Act [October 2, 1997].

Appendix D

The following is a paragraph regarding “transnational terrorism”.

When a terrorist incident in one country involves victims, targets, institutions, governments, or citizens of another country, terrorism assumes a *transnational* character. In the World Trade Center tragedy, citizens from over 80 countries lost their lives at the hands of terrorists who crossed into the United States from abroad. Obviously, the four hijackings on 11 September constitute transnational terrorist attacks. The kidnappings of foreigners in Lebanon during the 1980s, as a protest against Israeli-occupied territory, also represent transnational terrorism. Transnational terrorist incidents are *transboundary externalities*, insofar as actions conducted by terrorists or authorities in one country may impose uncompensated costs or benefits on people or property of another country. As such, myriad market failures are associated with collective actions to curb international terrorism.

This is from “An Economic Perspective on Transnational Terrorism” that can be found here: http://www.ecaar.org/Articles/SandlerDIW.pdf.

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401**	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS