I ask for your prompt attention to the following questions, which relate to...reports that force-on-force exercises at DOE facilities designed to test the adequacy of security have resulted in the mock "terrorists" successfully penetrating the facility and gaining access to sensitive nuclear materials more than 50% of the time. (The statement is also repeated on page 6 of the Markey letter.)

DOE categorically rejects the 50% figure for successful mock "terrorist" actions as representative of performance testing results for force-on-force tests conducted by DOE or DOE contractors. Indeed, the very concept of a "win/lose" percentage for such testing reflects a profound misunderstanding of the way in which DOE uses force-on-force performance testing, a misunderstanding that trivializes the real value of such testing.

The 50% figure has gained wide currency as a result of allegations first presented in a report by the private Project on Government Oversight (POGO). The figure, however, has no basis in DOE documentation of performance test results. DOE does not compile "win/lose" statistics on a Departmental basis. Force-on-force testing is used instead to evaluate discrete elements of protective force performance, such as individual and team tactics, command, control, and communications, and tactical response planning. DOE believes that there are strong reasons why trying to use simple "wins" and "losses" is of little value.

Force-on-force performance tests are conducted at DOE facilities for a number of different reasons. Many tests are conducted to evaluate proposed changes in protection strategies or in protective force tactical response plans. As such, these tests do not, by definition, test the adequacy of security itself. In many instances, including some tests at Rocky Flats and the Office of Transportation Safeguards that were referenced in the POGO report, the results of the test indicated that the proposed change was unwise, which meant that the tactical response configuration tested was never implemented at the site in question. In other instances, a less-than-satisfactory test result led to revisions in the proposed changes that were then tested successfully and implemented. Other force-on-force activities are conducted purely as training exercises, and may include alterations to the standard protection posture to enhance the effectiveness/efficiency of the training resources devoted to the test.

Finally, force-on-force tests are frequently conducted in conjunction with the process of validation and verification (V&V) of a site's Site Safeguards and Security Plan (SSSP). Although so-called V&V testing is often regarded as testing the adequacy of existing protection levels, it is typically an iterative process that actually serves the development and implementation of response plan revisions for a SSSP that is in process. Much V&V testing resembles the process described in the previous paragraph, in which changes being considered for inclusion in the upcoming SSSP are tested and adjustments are made in the plan's proposed protection strategy. Once these changes are assimilated, a final series of V&V tests are used to test the adequacy of the plan that will be presented to senior management for approval. Thus, it is typically only the final set of V&V tests conducted in support of a SSSP that are conducted against a final configuration of the site's protection strategy. Only these tests may be regarded as testing the adequacy of the site's actual protection effectiveness. Furthermore, even in the event that these final V&V tests reveal a weakness in protection, sites are expected to correct that weakness and retest before the SSSP is approved.

In addition to this final set of V&V tests, there are two other categories of force-on-force performance testing that may be regarded as testing the adequacy of security at a facility. These

are (1) the tests conducted by OA as part of its program of inspections at DOE sites, and (2) tests conducted by the site in fulfillment of the annual requirement to verify the effectiveness of critical security system elements. (The latter tests are frequently carried out with the support/participation of the supervising DOE field and Headquarters organizations and frequently are conducted in conjunction with surveys of overall program effectiveness.)

Even in the case of these tests, however, it is totally misleading to attempt to draw simple "win/lose" conclusions, for several reasons. First, for safety and security reasons, artificialities abound in even the most realistic tests. Although these artificialities do not invalidate the use of test results in evaluating such things as individual and team tactics or command and control, they argue strongly against treating apparent successes in penetrating to a target as reflecting the actual likelihood that a real adversary might successfully apply the same scenario. Second, the number of tests performed in even the most extensive testing program *never* rises to the level of statistical certainty for any given attack scenario.

For example, when OA conducts force-on-force performance tests as part of a safeguards and security inspection, it typically conducts a maximum of four such tests for a given inspection. This number represents the most that can be conducted given the available time and personnel resources. Usually, the four tests involve different scenarios aimed at different target locations, in order to assure that the inspectors have the greatest opportunity to observe protective force tactics and response plans under the widest variety of stressful circumstances. This means that, at most, for any typical inspection, there is only one test of a particular scenario/target combination. To argue that a single "win" or "loss" in such circumstances should be taken as indicative of overall protection effectiveness flies in the face of reason. It is precisely for this reason that OA uses such performance testing as only a single element in a much larger program of testing and evaluation activities in reaching its conclusions about protection system effectiveness, conclusions that are reflected in the ratings assigned for each inspection.

Page 3, Question: In light of potentially devastating consequences of a successful terrorist attack on a DOE nuclear facility, and in light of recent evidence that Al Qaeda members are seeking to commit acts of terrorism involving nuclear materials, I ask for your prompt attention to the following questions, which relate to:

Whether the Design Basis Threat for DOE facilities, which defines the threat level against which the facilities must be protected, is realistic in light of the events of September 11 and information regarding Al Qaeda's desire to acquire nuclear materials or attack U.S. nuclear facilities.

Answer: Based on the events of September 11, 2001, the DOE, in cooperation with the Department of Defense (DOD), recognized that a revised interim threat statement must be developed. Consequently, the DOE and DOD have developed a draft "Interim Joint Threat Policy Statement" (IJTPS) which specifically addresses the events of September 11, 2001. The IJTPS is in review and comment in the DOE and DOD as of May 2002. It is anticipated that the IJTPS will be finalized during the Summer 2002. The formal DOE DBT is derived from the Postulated Threat developed by the U.S. intelligence community. The Postulated Threat data-gathering phase, which considers the events of September 11, 2001, is in process. The first draft of the Postulated Threat is scheduled for late Spring 2002. The final Postulated Threat is scheduled for release in the Fall 2002. The DOE DBT is began development May 2002. The official DOE DBT is scheduled to be issued within 90 days of the official Postulated Threat.

SECTION: Questions Related to DOE's Responses to the Events of September 11

Page 4, Question 5: A recent news report stated that a DOE program that trains foreign nationals to, among other things, identify holes in modern security systems trained students fromYemen, the Phillippines, Kenya and other countries. These students reportedly enrolled in classes at Kirtland Air Force Base in New Mexico and "interfaced" with security teams at Sandia National Laboratories. The reported purpose of the course was to teach the students how to protect a facility and determine its vulnerabilities. I am concerned that if this report is true, that the existence of this program could have the unintended consequence of teaching future terrorists how to penetrate U.S. security systems.

a: Please fully describe the nature and purpose of this program. Are these individuals being trained in the use of the ASSESS program, which is used to determine risk and vulnerabilities at a nuclear site? What access are foreign nationals participating in this program given to databases containing information related to the effectiveness of the security components, such as alarms, barriers, vendors of these systems, etc.?

Answer: The Antiterrorism Program (ATAP) is a U.S. Department of State program. The program is designed to assist in protecting U.S. embassies, military bases, businesses and tourists abroad. The Department of State (DOS) and the Department of Energy (DOE) entered into an Interagency Agreement under the Economy in Government Act for the DOE to provide training assistance to the DOS.

The Department of State Bureau of Diplomatic Security Service, Antiterrorism Assistance Program – Vital Installation Security (VIS) course is designed to assist delegations of foreign countries to harden their facilities to the many threats. One of these is the threat posed by the terrorist. Information in this course has a heavy emphasis on physical security systems, with additional topical areas covering contingency planning, terrorist methodology, non-technical perimeter security, incident command, and the supervisory role in handling incidents involving explosive ordinance. The members of the foreign delegations participating in this program are members of their National Police forces, and other associated police agencies.

Delegations participating in the VIS program are being taught security principles accepted by the international industrial security community. Information taught in the physical security topical areas is extrapolated from open source resources. Most of these resources are accepted by and are endorsed by the American Society for Industrial Security. The core of the physical security topical areas draw their content from resources including: The Protection of Assets Manual (Merritt Publishing), Risk Analysis and the Security Survey (by James Broder) and Security 101 (by Senstar Stellar).

The delegations participating in the VIS program are not given access to any DOE sensitive or classified material. Delegations are not given any training on the ASSESS software, nor are they provided access to any DOE or other government databases containing information on system vulnerabilities or effectiveness.

As a part of the training for this program, delegations are provided information that vendors usually provide to the international community. This includes brochures and handout material concerning various physical security systems the vendors supply.

Page 5, Question 5b: Prior to September 11, please describe the measures taken to ensure that the students were not members of foreign or domestic groups that seek to do harm to the U.S. Did they undergo security background checks, if not, why not?

Page 5, Question 5d: Have any of these classes been run after September 11? If so, did those participants undergo security background checks to ensure that they were not members of domestic or foreign groups that seek to do harm to the U.S.

Page 5, Question 5h: A registration form for a similar (or possibly identical) course offered by CH2m Hill, also at Sandia National Laboratories (see http://www.ch2m.com/flash/Services/competencies/PhysicalSecurity/Security Training/assets/registration_form.pdf) does not even ask for information such as country of citizenship, immigration status or social security number. How can you be sure that members of Al Qeada have not and are not currently enrolled in these courses?

Answer to 5b, 5d and 5h: Since September 11, there have been two iterations of the VIS program. All delegates from these countries, prior to September 11 and since September 11, are screened by the American Embassy within the delegates' country. The countries and delegates selected to attend courses in Albuquerque, and in other locations in the US, are chosen and screened by the Department of State. Delegates are processed in accordance with DOE requirements for foreign visitors and put into the Foreign Access Central Tracking System (FACTS) database, which feeds into the U.S. Counterintelligence Analytical and Research System (CARDS).

The form for which information is collected for entry into the non-sensitive DOE facility is SF 7643-IFN (07-2001). This form requires the following information for each delegate:
Name
Rank
Employment information (Name of employer, address, phone number)
Permanent address
Date and place of birth
Country of citizenship
Passport number and expiration date
VISA type and expiration date
Social Security Number

Page 5, Question 5e: The press report indicates that a number of Yemeni students who completed the course subsequently disappeared. Is this true? If so, what has been done to locate them?

Answer: Two members of the delegation from Yemen disappeared at the conclusion of the VIS program. The FBI, Department of State and Department of Energy were notified immediately of this incident. The FBI took responsibility for the investigation upon notification.

Page 5, Question 5f: Do you intend to continue this course? If so, why, given the potential threat it could pose to national security?

Answer: Considering the international threat posed by terrorism, it is even more imperative this course continue. The war on terrorism is not fought on a singular front, it requires attacks from all sides as well as defensive measures. Military strategists, both present and historical, would all agree that it is imperative to harden potential targets against the terrorist threat. This process of hardening comes partially through the training given by the Vital Installation Program.

Upon close scrutiny, it rapidly becomes apparent, that there is a greater threat to National Security if the terrorist threat in other countries is allowed to succeed. A prime example of this concept is the events surrounding September 11.

National security is of paramount importance, as is the security of American citizens and delegations around the world. The Department of State has stated there has been numerous incidents in which American lives were saved as a result of this and other similar programs.

Many of the countries that have given the U.S. permission to establish ground bases have sent delegations to this course. It is possible that part of their cooperativeness rests on some of the rapport established with the Americans who were responsible for providing instruction in this and similar courses.

Page 5, Question 5g: Before September 11, did you consider this program to be sensitive or non-sensitive? What about after September 11?

Answer: This program has always been treated as sensitive, in that the material presented is targeted toward law enforcement agencies. As this program deals with terrorism on an international scale, the attack on September 11 only adds to the serious nature of the material being taught. For those law enforcement officers within the U.S. who elect to participate in this program, they as well as the delegates of foreign governments are taught on an international level, with an emphasis of bringing the information into a format that can be used and applied to the specific country.

Question 5c): It is my understanding that DOE classified countries as being sensitive or non-sensitive. Please explain how citizens of each country classification would be examined prior to being allowed to enroll in this program. What was Afghanistan's classification prior to September 11? Has it changed since then and if so, when? Please provide a list of all countries DOE considers to be sensitive.

DOE developed its Sensitive Country List (attached) as a tool to be used in connection with the DOE Foreign National Visits and Assignments Program and the DOE Foreign Travel Program.

Proposed visits to DOE facilities by foreign nationals from countries on the list are reviewed by the Office of Counterintelligence as part of the overall review and approval process. The overall review determines not only whether the visit will take place but also the degree of access the foreign national may have to DOE technology, equipment, or materials and the requirements for supervision or escort of the foreign national. The review also determines whether the visit involves technology subject to Department of Commerce, Department of State or DOE export licensing.

Proposed foreign travel by DOE employees to sensitive list countries also is reviewed by the Office of Counterintelligence as part of the overall review process. The overall review determines not only whether the travel will take place but also requirements for briefing the DOE traveler about potential security concerns associated with the trip.

Afghanistan was never on the sensitive country list because the U.S. Government did not recognize the Taliban regime as the Government of Afghanistan. In any case, no Afghan national has participated in the ATAP/VIS course described above.

DOE SENSITIVE COUNTRY LIST - July 1999

Current through November 2000

Countries appear on this list for reasons of national security, terrorism, or nuclear proliferation support. This list is also used in implementing DOE Order 1240.2B, "Unclassified Visits and Assignments by Foreign Nationals" and DOE Order 1500, "Foreign Travel Authorization."

Algeria
Armenia
Azerbaijan
Belarus
China, People's Republic of
Cuba
Georgia
India
Iran
Iraq
Israel
Kazakstan
Kyrgyzstan
Libya
Moldova
North Korea, Democratic People's Republic of
Pakistan
Russia
Sudan
Syria
Taiwan
Tajikistan
Turkmenistan
Ukraine
Uzbekistan

Page 6, Question #6: The 1998 letter sent to me by then-DOE Secretary Pena stated that "the FBI does not routinely search names of all DOE employees and provide information to DOE concerning those employees." Was this policy still in effect on September 11? What about after September 11? Don't you think that it would be a good idea to ensure that none of the U.S. or foreign nationals currently working at DOE facilities belong to domestic or foreign groups that seek to harm the U.S.? If not, why not?

DOE Personnel Security policy has always included FBI indices checks as part of the investigations conducted on all individuals who are processed for an access authorization (security clearance). These checks include the FBI fingerprint database (FBIF), the FBI fingerprint name index (FBFN) and the FBI records of investigations (FBIN) which covers background, criminal, loyalty and intelligence investigations conducted by the FBI. These same indices are checked for all newly-hired DOE Federal employees who do not require access authorization as part of the suitability investigation that the DOE Office of Personnel is required to conduct. Once an individual has been recorded in the FBI database as having been a DOE access authorization applicant, DOE will be notified of any arrests that are reported to the FBI by an arresting agency.

Page 6, question 7: Has Rocky Flats processed any nuclear materials on the main floor since September 11? If so, do you believe this was in accordance with the heightened security measures in effect?

The question does not specify a particular building (i.e., the Plutonium Stabilization and Packaging System, Building 371); however, nuclear material has been processed at Rocky Flats since September 11, 2001. Additionally, all nuclear material processing after September 11, 2001 has been in accordance with the heightened security requirements.

SECTION: Questions Related to DOE's Response to the Events of September 11

Page 6, Question 8: What is DOE's definition of "adequate" security? Is it an absolute measure based on the outcome of force-on-force exercises and vulnerability analyses, or a relative measure based on how much a particular facility has improved its security?

Answer: The DOE has established safeguards and security programs designed to ensure appropriate safeguards and security protection postures at DOE facilities. The safeguards and security program contain both compliance based elements and performance based elements. A DOE facility is required to meet the compliance based criteria as detailed by DOE Orders and the performance based criteria as detailed in the DOE risk management process (as embodied in the Site Safeguards and Security Plan (SSSP) program).

The compliance based programs are inspected and evaluated by various entities to ensure execution of the DOE Orders and Manuals. The reviews of the compliance based programs are accomplished by: self-assessments by the contractor, safeguards and security surveys by the area/field office, inspections and evaluations by the Office of Safeguards and Security Evaluations, and safeguards and security audits by interested parties (i.e., Office of the Inspector General, General Accounting Office).

The DOE risk management process is embodied in the SSSP program. The SSSP vulnerability assessment process utilizes computer modeling, computer-based engagement simulations, expert judgment, performance testing and force-on-force exercises to assess the safeguards and security protection posture. These tools and programs ensure protection is afforded to DOE assets.

The aggregate of the compliance based and performance based safeguards and security programs at a DOE facility determines the overall "adequacy" of the site safeguards and security protection posture.

SECTION: Questions Related to DOE's Response to the Events of September 11

Page 6, Question 9: A December 15, 2001 press release from the Nuclear Control Institute states that the Defense Nuclear Facilities Safely Board (DNFSB), an independent board charged with overseeing safety at DOE facilities, was instructed by DOE not to release any documents in response to public inquiries. While I agree that all Federal agencies should be careful not to release any national security information, it is vital that the activities of the government should remain as open and transparent as possible to the public.

a: Is it true that DOE has instructed the DNFSB not to release any documents to the public, even if they don't contain classified material, and if so, why?

Answer: The Deputy Secretary requested in writing that the DNFSB review Departmental information held by the DNFSB and publicly available for potential impact to DOE security operations. Subsequent correspondence and communication with the DNFSB resulted in DOE (NNSA) providing a request to the DNFSB with a list of documents to be reviewed for security relevant impact. The Department also requested that the DNFSB remove the suspect documents from public access until they had been reviewed and a determination made on potential impacts to Departmental security operations.

A preliminary review of the suspect documents determined that they contained information that an adversary could use to defeat the security forces at specific facilities. In some cases this information was provided in excess of regulatory requirements for the release of safety and environmental impact information. In all cases, the security relevant information is not eligible for classification under Executive Order 12958, "National Security Information" or the Atomic Energy Act of 1954, as amended. As demonstrated by the events of September 11, 2001, the threat to domestic locations has changed. With this change in threat, the context in which information relating to facility and security operations has changed. In order for the Department to fulfill its obligations of due diligence with regards to public safety, environmental issues, and security, a conservative approach has been taken to re-evaluate selected information documents in the public domain.

Existing documents and information are being reviewed as quickly as resources allow. If possible, the documents are sanitized to remove specific security relevant information and then placed back in the public domain. If sanitization is not required or if the information cannot be removed without impacting the purpose of the document, then the document is placed back the public domain with no modification. New documents are reviewed to ensure that security relevant information is not released prior to placement in the public domain.

Page 6, Question 9b: When does DOE intend to resume its release of all appropriate documentation to the public?

Answer: On October 26, 2001, Deputy Secretary Francis S. Blake issued a memorandum to all departmental elements directing Departmental Elements to review publicly available information

in light of the terrorist events of September 11, 2001. Specifically, this review directed that all departmental elements review operational information that has been made accessible to the public, and to remove or restrict access, as appropriate, to information that may be used to target the Department of Energy. A copy of this memorandum has been included for your information.

In order to facilitate this directive, the Safeguards and Security Policy Staff, Office of Security, chaired a working group to develop a process and guidelines that programmatic elements of the Department could use to implement the Deputy Secretary's direction. The Safeguards and Security Policy staff recommended that Departmental sites and organizations engage the existing operational security (OPSEC) resources at local sites to facilitate the review of publicly available information in order to identify information that would be of assistance to potential adversaries. Once the information was identified, local management would be provided with recommendations concerning the risks of leaving suspect information in the public domain vs. the need to inform local communities of activities at Departmental sites. Depending on the local decisions, the suspect information remained in the public domain and was mitigated by other security measures, or the suspect information was removed from the public domain. Departmental guidance was developed to assist local management in balancing the need to inform the public vs. increasing the threat and risk at specific facilities. A copy of the guidance provided by the Safeguards and Security Policy staff during an Interactive Television Broadcast on web content review has also been included for your information.

The Department's goal is to provide as much relevant information to the public, especially with regards to Environmental Impact Statements and Safety Analysis Reports, as possible without providing increased knowledge to potential adversaries that would be used to defeat local site security. Existing documents and information are being reviewed as quickly as resources allow. If possible, the documents are sanitized to remove specific security relevant information and then placed back in the public domain. If sanitization is not required or if the information cannot be removed without impacting the purpose of the document, then the document is placed back the public domain with no modification. New documents are reviewed to ensure that security relevant information is not released prior to placement in the public domain.

Assessing Information on DOE Web Sites

BACKGROUND:

Information on DOE web sites may be of benefit to those who may (a) target DOE facilities or sites for terrorist attacks, (b) use the information to develop weapons of mass destruction, or (c) otherwise commit acts detrimental to U.S. national security, citizens, or property. In order to disrupt or deny these potential activities, the information contained on DOE web sites must be assessed in order to determine its sensitivity and the risk to U.S. and Department interests if the information is allowed to remain in the public domain. If there is some doubt as to the risk, it is better to remove the information rather than to leave it where it can be easily accessed.

PROCEDURE:

A list of the types of information that should be considered for removal from DOE web sites is attached. The information can be found in numerous type documents. The driving factor for the examination of data contained on web sites should be the risk posed by the easy access to the information afforded by its being placed on the Internet. For example, a detailed map of a facility showing the location of stored nuclear waste could be of great interest to a terrorist. If there is reason (public law or agreement) for the public to be able to access this information, the next consideration should be how the requirement for public access can be met and still restrict the access to the information. In many, if not all, cases this can be done by placing the information in a reading room and requiring the presentation of some form of identification before access is granted. The information can then be removed from the web site.

In determining the risk to leaving the information on the Internet personnel must assume the role of the adversary, in this case the terrorist. All avenues of possible use must be explored. Remember, until September 11th, no one thought of using commercial jet planes as flying bombs, except for the terrorist.

The Department's Operations Security (OPSEC) program is designed to accomplish the task considering the sensitivity of information and the risk posed by placing data where it is easily accessible. If your particular organization does not have an OPSEC program, contact someone in your parent organization who does or contact the DOE OPSEC Program Manager, Greg Griffin, at (301) 903-3653 for assistance.

Potentially Sensitive Information on DOE Web Sites

These items are to be used in considering whether or not information should be on *publicly accessible* web sites.

Facilities

- Description and location of Facilities to include maps, written directions, drawings, blue prints, photographs and the like
- Descriptions and location of storage facilities for nuclear or other hazardous materials
- Descriptions and location of personnel or facility support systems (e.g., water supply, electrical supply systems, communications systems, emergency response personnel/equipment)
- Descriptions and locations of computer systems used to process, store, and transmit sensitive information.
- Environmental Impact Statements
- Any information pertaining to other sites that has not been reviewed/approved by the other site.

Materials

- Form and quantity of hazardous materials (chemical, nuclear, biological)
- Vulnerabilities of materials to unauthorized access or destruction
- Consequences of release of hazardous materials
- Transportation related information (routes, maps, shipping means, containers)

Security/Safety

- Plans, procedures, communications, reaction times, capabilities
- Assessments, exercise results, evaluations
- Personnel data identifying security/safety personnel
- Equipment

Assessments

- Vulnerability assessments
- Safety assessments/analysis
- Risk analyses
- Hazardous assessments (Dispersion models and analyses, accident analyses)

Personnel

- Organization charts, phone lists identifying senior management/key personnel
- Personal data to include travel plans, meetings and the like
- Training materials that include sensitive information

Programs

- Information identifying sensitive programs, special projects, SAPs, WFO
- Reports detailing activities and/or results from programs and projects
- Information pertaining to programs at other facilities/sites that has not been cleared with the other sites for publication on a publically accessible web site.

Safeguards and Security Policy Staff

Web Information Review Process

Introduction

We have entered the Information Age. Information is rapidly becoming the "coin of the realm" and is sought by everyone. The information residing on automated information systems is a significant representation of the lifeblood of the agency, business, or organization involved, and collectively, the lifeblood of this country. Furthermore, the growth of the Internet has made information even more accessible. The Department has a wealth of information and makes full use of the Internet to make its information available to the public. This accessibility can be a two edged sword, however. Our adversaries can also access our information and use it to the detriment of the United States, its citizens, and its guests.

The events of September 11th have clearly demonstrated that terrorists will go to any means to attempt to accomplish their purpose. It is therefore incumbent on DOE to ensure that information that might aid terrorist organizations is given protection commensurate with the risk involved in its access by terrorist organizations. The process given in this guide is designed to reduce the possibility that sensitive information of use to a terrorist is placed on DOE-sponsored web sites where it can be easily and anonymously accessed.

Process

Most facilities have at least one office or individual who is responsible for placing information on the World Wide Web. Before any information is placed on a web site it should be reviewed for three factors:

- ✓ Suitability-Is it suitable for distribution by the organization publishing it and is it suitable for public distribution.
- ✓ Sensitivity-If published on the Internet, could this information identify possible links to sensitive activities or programs.
- ✓ Risk-Could the information be used by terrorists to the detriment of the United States and if so, what is the risk involved if the information is published on the Internet.

A proven technique for the conduct of the information review is to establish a group responsible for the review.

Review Team Composition

At a minimum the review team should consist of the person(s) responsible for placing information on a web site, a member from the program of interest, a representative from the Operations Security (OPSEC) program, and a representative from the local Counterintelligence (CI) Office.

The determination of the suitability should be accomplished by either the office or individual with the responsibility for seeing that the information is placed on a web site. Does it present the type of image that the Department wants to project to the general public? The originating office may have a review process in place and, if so, can certify that this requirement has been met.

The information should be reviewed by the OPSEC manager or a member of the OPSEC working group for its sensitivity. The sensitivity depends on the use that can be made of the information and its ease of access. If the information has already been released into the public domain by other means, then the requirement not to publish it is lessened. Care must also be taken to determine whether or not the information might disclose a sensitive program or activity. In making this determination it is necessary to remember that the aggregation of information can often be used to identify classified or sensitive unclassified activities and programs.

The risk of the information being of value to a terrorist or other adversary must also be determined. Many times those involved in the counterintelligence program can provide valuable insight into this factor. If it is deemed to be of no value to a terrorist, then again the requirement to not publish may be lessened. In determining its potential value to a terrorist or other adversary care must be taken to examine all potential uses of the information, even uses that may seem extreme. Remember, until September 11th no one considered the use of a commercial flight as a flying bomb but it was an effective use.

The review itself can either be accomplished in a group or individually. The important factor is that all information should be subject to a review before it is published on the Internet. Depending on the size of the organization involved one or more review groups can be established. Use of separate groups within a large organization permits each group to focus on its area of expertise.

Summary

The Internet is an unbelievable source of information. It can be accessed electronically and anonymously. That the Department has had sensitive information placed on web sites is indicated by Internet assessments that have been conducted. One such assessment managed to produce a classified document from information gathered from the Internet. The terrorist activity of September 11th has shown that the United States could be the site of more such activities. The Department has information that could be used by terrorists for these activities. It is incumbent on all concerned to try and ensure that such information is not easily available to them.

28

The Deputy Secretary of Energy
Washington, DC 20585

October 26, 2001

MEMORANDUM FOR ALL DEPARTMENTAL ELEMENTS

FROM: FRANCIS S. BLAKE

SUBJECT: Reviewing the Availability of Operational Information

The recent terrorist attacks have heightened our concern regarding publicly available information about the operations of the Department's sites, facilities, and activities. Some operational information which may be available through Internet web sites and other venues could be used by those who target our sites, facilities, and activities for terrorist attacks. Examples of such information include: emergency planning hazards assessments; safety analysis reports; environmental impact statements; detailed site/facility maps; photographs of facilities; and personal data on Federal and contractor employees.

Immediately upon receipt of this memorandum, please review the operational information accessible to members of the public and remove or restrict access, as appropriate, to information that may be used to target the Department of Energy. Please provide a summary of this review and your actions to Mr. Joseph S. Mahaley, Director, Office of Security and Emergency Operations, within 15 days of the date of this memorandum.

Questions may be directed to Mr. Mahaley at (202) 586-3345 or via e-mail at Joseph.Mahaley@hq.doe.gov. Thank you for your immediate attention and action.

Printed with soy ink on recycled paper

John T. Conway, Chairman
A.J. Eggenberger, Vice Chairman
Joseph J. DiNunno
John E. Mansfield

DEFENSE NUCLEAR FACILITIES SAFETY BOARD

625 Indiana Avenue, NW, Suite 700, Washington, D.C. 20004-2901
(202) 694-7000

December 4, 2001

The Honorable Francis S. Blake
Deputy Secretary of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1000

Dear Mr. Blake:

The Defense Nuclear Facilities Safety Board (Board) shares the concern for national security expressed in your letter dated November 14, 2001. The Board has cooperated, and will continue to cooperate, with the Department of Energy (DOE) and others to ensure that access to harmful information is denied to adversaries of the United States. We will respond promptly and effectively to any guidance provided on this topic.

Your letter suggests that the Board should develop in-house expertise to administer a new category of sensitive, but not classified, information. The parameters of this category are suggested–but not yet fully defined–by the list attached to your letter. Documents covered by this category range from the highly specific to the very general. Your letter offers to provide training to Board personnel "generating reports and documents so that they do not contain information potentially useful to terrorists."

The Board does not have the authority to make determinations regarding release of information potentially harmful to the common defense and security of the United States. Section 2286d(h) of the Board's organic statute states that the requirement to make information available to the public "shall not apply in the case of information that is classified" and "shall be subject to the orders and regulations issued by the Secretary of Energy under sections 2167 and 2168 [§§147 and 148 of the Atomic Energy Act] to prohibit dissemination of certain information." The Board reads this statutory provision as an indication of Congressional intent that the Board is not to make independent decisions on the release of any information affecting national security.

Therefore, the Board plans to continue its current practice of sending Board-generated documents to DOE for classification review, with the expectation that DOE will also review these documents for sensitive information that may fall within the new categories identified in your letter. We request that DOE identify any such sensitive information by marking these documents, similarly to the classification markings, as releasable in their entirety, partially

releasable with redactions indicated, or not to be released. The Board will protect each document as marked, and will consult with DOE if a request is received for the document under the Freedom of Information Act. The Board will also consult with DOE prior to releasing documents already in our files but not reviewed by DOE under the new guidelines you have provided.

Please contact me if you have any questions.

Sincerely,

John T. Conway
Chairman

c. Mark B. Whitaker, Jr.