

SAIC.txt

Subject: Comments on the Implementation of Section 214 of Title II, Subtitle B, of the Homeland Security Act

Date: Fri, 13 Jun 2003 17:15:20 -0400

From: "Casciano, John P." <JOHN.P.CASCIANO@saic.com>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

CC: "Suzanne Gorman (E-mail)" <sgorman@siac.com>,
"Bobby R. Gillham (E-mail)" <bobby.r.gillham@conocophillips.com>,
"Kendra L. Martin (E-mail)" <martink@api.org>

Please see the attached cover letter and comments. We will mail paper copies as well. Thank you for your consideration. John Casciano, Senior Vice President, Enterprise Security Solutions Group, Science Applications International Corporation (SAIC).

<<SAIC - Cover Letter for Critical Infrastructure Commentsv2.doc>>
<<SAIC - Critical Infrastructure Comments on Rulemaking v3.doc>>

Cover Letter
Critical
Infrastructure
Commentsv2.doc
WINWORD File
SAIC - Cover Letter for Critical Infrastructure Commentsv2.doc
(application/msword)

Name: SAIC -
for
Type:
Encoding: base64
Description: SAIC -

Cover Letter
Critical
Infrastructure
Commentsv2.doc

for

Critical
Infrastructure
on
Rulemaking v3.doc
File
SAIC - Critical Infrastructure Comments on Rulemaking v3.doc
(application/msword)

Name: SAIC -
Comments
Type: WINWORD
Encoding: base64
Description: SAIC -

Critical
Infrastructure
on
Rulemaking v3.doc

Comments

June 12, 2003

Associate General Counsel
General Law
Department of Homeland Security
Washington, DC 20528

Dear Associate General Counsel:

Pursuant to the April 15, 2003 *Federal Register* Notice of Proposed Rulemaking for Procedures for Handling Critical Infrastructure Information, enclosed is an original and three copies of comments submitted on behalf of the Enterprise Security Solutions Group (ESSG) of Science Applications International Corporation (SAIC), a Fortune 500 Company. As a point of reference, ESSG is SAIC's Center of Cybersecurity expertise and as such provides 24x7 services to the Energy, Financial Services, Worldwide, Canadian, and Japan Information Sharing and Analysis Centers (ISAC). Copies of these comments are being provided for information to the Financial Services and Energy ISACs.

Should you desire to discuss these comments, please either contact either the undersigned at 703-375-2013, or Ms Jody R. Westby, Esq. at 720-570-1403.

Respectfully submitted,

John P. Casciano
Group Senior Vice President, Group Manager
Enterprise Security Solutions Group

Enclosures

**BEFORE THE
DEPARTMENT OF HOMELAND SECURITY**

**In the Matter Of
Implementation of Section 214 of Title II, Subtitle B, of the Homeland Security Act
Procedures for Handling Critical Infrastructure Protection**

RIN 1601-AA14

**Comments of
Science Applications International Corporation (SAIC)
Enterprise Security Solutions Group**

**John P. Casciano
Group Senior Vice President
Enterprise Security Solutions Group
SAIC
12100 Sunset Hills Road
Second Floor, M/S REC 2-1
Reston, VA 20190
(703) 375-2013
(703) 375-2085 – fax**

Prepared by: Jody R. Westby, Esq.

June 16, 2003

TABLE OF CONTENTS

	<u>Page</u>
SUMMARY.....	3
I. Introduction.....	4
II. The lack of a clear explanation in the rules of the terms “critical infrastructure” and “protected systems” undermines the purpose of the Act and leaves uncertainty regarding the protection of shared information and its exemption from Freedom of Information Act (FOIA) disclosures.....	5
III. To reduce uncertainties, a procedure should be established in the rule to allow companies to receive an advanced determination from DHS regarding whether specific systems qualify as critical infrastructure or protected systems.....	17
IV. Even if information is protected as information pertaining to critical infrastructure or protected systems, gaping holes in the protection of this information significantly weaken this protection through its allowed use in criminal investigations and prosecutions and its disclosure to Congress and the GAO without (a) written precautions against further disclosure and (b) notification to the submitting party.....	17
V. Sharing critical infrastructure information with foreign governments as provided in Sections 29.1(a)(4), 29.1(b), and 29.8(j) of the proposed rule is not authorized by the Act and introduces serious uncertainties into the information sharing atmosphere.....	18
VI. The source of shared information should be more specifically protected in the CII database by encrypting identifying information or using a tracking or identification number assigned to the submitting party.....	19
VII. Although no private right of action is provided by the Act, the rules should establish a procedure for addressing, and potentially investigating, grievances or complaints regarding the manner in which shared information was handled and protected.....	20
VIII. Conclusion.....	20

SUMMARY

In these comments, the Enterprise Security Solutions Group of Science Applications International Corporation (SAIC) responds to the Department of Homeland Security's Notice of Proposed Rulemaking on Procedures for Handling Critical Infrastructure Information. Our comments address six areas of concern and we offer concrete suggestions for each:

1. The lack of a clear explanation in the rule of the terms “critical infrastructure” and “protected systems” undermines the purpose of Section 214 of the Homeland Security Act of 2002 (Act) and creates uncertainty regarding the protection afforded shared information and its exemption from FOIA.

Recommendation

We recommend the rule be amended to more clearly delineate through description and example (a) what “systems and assets” are included within the term “critical infrastructure,” (b) what types of systems would be considered “protected systems,” and (c) of these, which are considered “so vital to the United States” that the incapacity or destruction of these systems and assets would have a debilitating impact.

2. The rule does not provide any certainty prior to the sharing of information whether that information will be protected.

Recommendation

We recommend the rule include a procedure that would enable organizations to obtain an advance determination from the CII Program Manager of whether their system(s) qualify as “critical infrastructure” or “protected systems” to allow them to know if information shared regarding those systems would be protected and exempt from FOIA.

3. Even if information is protected, gaping holes in the protection of this information exist through the allowed use of this information in criminal investigations and prosecutions and its disclosure to Congress and the GAO.

Recommendation

We recommend the rule be amended to include a notice of disclosure to the submitting party of such use or disclosure and that the rule require a notice be visibly attached to the information which informs the receiving entity that the information is Protected Critical Infrastructure Information (Protected CII) and advises against further disclosure. We believe these two requirements would prevent widespread dissemination of the information and would instill greater confidence in the CII Program.

4. The sharing of Protected CII with foreign governments as provided in Sections 29.1(a), 29.1(b), and 29.8(j) of the proposed rule is not authorized by the Act and introduces serious uncertainties into the information sharing atmosphere.

Recommendation

We recommend these references to sharing Protected CII be stricken from the proposed rule because they are not authorized by the Act.

5. The source of shared information should be more specifically protected in the CII database.

Recommendation

We recommend that the proposed rule require the name of the submitting entity in the database to be either encrypted or replaced by a tracking or identification number that is assigned to the submitting party.

6. Although no private right of action is provided by the Act, the rules should establish a procedure for addressing, and potentially investigating, grievances or complaints regarding the manner in which shared information was handled or protected.

Recommendation

We recommend the rule be amended to include a simple complaint/grievance procedure to (a) enable a better public-private exchange regarding the operations of the CII Program, (b) provide a mechanism for addressing the concerns of the submitting parties, and (c) help the CII Program become more user-friendly and trusted.

I. Introduction

The Enterprise Security Solutions Group of Science Applications International Corporation (SAIC) respectfully submits these comments to the Department of Homeland Security (DHS) on its notice of proposed rulemaking¹ to establish uniform procedures to implement Section 214 of the Homeland Security Act of 2002² (Act) regarding the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal Government.

SAIC offers comments on the following issues to assist DHS in finalizing the proposed rule.

1. The lack of a clear explanation in the rules of the terms “critical infrastructure” and “protected systems” undermines the purpose of the Act and leaves uncertainty regarding

the protection of shared information and its exemption from Freedom of Information Act (FOIA) disclosures.

2. To reduce uncertainties, a procedure should be established in the rule to allow companies to receive an advanced determination from DHS regarding whether specific systems qualify as critical infrastructure or protected systems.
3. Even if information is protected as information pertaining to critical infrastructure or protected systems, gaping holes in the protection of this information significantly weaken this protection through its allowed use in criminal investigations and prosecutions and its disclosure to Congress and the GAO without (a) written precautions against further disclosure and (b) notification to the submitting party.
4. Sharing critical infrastructure information with foreign governments as provided in Sections 29.1(a)(4), 29.1(b), and 29.8(j) of the proposed rule is not authorized by the Act and introduces serious uncertainties into the information sharing atmosphere.
5. The source of shared information should be more specifically protected in the CII database by encrypting identifying information or using a tracking or identification number assigned to the submitting party.
6. Although no private right of action is provided by the Act, the rules should establish a procedure for addressing, and potentially investigating, grievances or complaints regarding the manner in which shared information was handled and protected.

II. The lack of a clear explanation in the rules of the terms “critical infrastructure” and “protected systems” undermines the purpose of the Act and leaves uncertainty regarding the protection of shared information and its exemption from Freedom of Information Act (FOIA) disclosures.

Background

Over the course of the past five years, the U.S. Government has engaged in an extended dialogue with industry and trade associations regarding companies' reluctance to report and share information regarding computer security incidents. This reluctance to share such information revolved around three concerns:

1. Companies feared that information shared with the Government might be disclosed through Freedom of Information Act (FOIA) requests.
2. Businesses worried that lack of protections for this information could result in the disclosure of confidential or proprietary information, harm to the submitting company's reputation, a loss of market share, or a drop in share price. Indeed, research has shown that when Yahoo!, Ebay, and Amazon.com were the victims of distributed denial of service attacks, they suffered a drop in the company stock price of 17-23% in the three weeks following the attack. This amounted to a \$4.56 billion loss in market capitalization for Ebay, a \$6.67 market cap loss for Amazon.com, and a \$17.24 billion drop for Yahoo!³
3. Companies were concerned that shared information would be used in criminal investigations that they would not have control over and which could significantly disrupt operations or cause other problems, including those enumerated in point 2 above.

The fear that information submitted to the Government might be subsequently disclosed through Freedom of Information Act (FOIA) requests was recognized by the Government and Congress as a clear deterrent to the sharing of corporate security incident information.

Prior to enactment of the Act, FOIA provided for specific exemptions to requests for the following types of information:

- (a) Information that was specifically authorized and classified under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy;
- (b) Information related solely to the internal personnel rules and practices of an agency;
- (c) Information specifically exempted by another statute that either requires the information to be withheld without discretion, establishes criteria for withholding the information, or refers to the particular types of matters to be withheld;
- (d) Trade secrets and commercial or financial information obtained from a person that is also privileged or confidential;
- (e) Inter-agency or intra-agency memoranda or letters that would not be available to a party other than an agency in litigation with another agency;
- (f) Personnel and medical files and similar information that would constitute a clear unwarranted invasion of personal privacy;
- (g) Records or information compiled for law enforcement purposes, but only to the extent that the production of such information could:
 - ◆ reasonably be expected to interfere with enforcement proceedings;
 - ◆ deprive a person of the right to a fair trial or an impartial hearing;
 - ◆ disclose the identity of a confidential source, including a state, local, or foreign agency or authority or any private institution;
 - ◆ disclose techniques and procedures for law enforcement investigations and prosecutions;
 - or
 - ◆ endanger the life or physical safety of any individual;
- (h) Records that pertain to examination, operation, or condition of financial institutions; or
- (i) Geological and geophysical information and data concerning oil wells and maps.⁴

The National Infrastructure Protection Center (NIPC), which was housed in the Federal Bureau of Investigation (FBI) and the Department of Justice (DOJ) and is now an entity within the Homeland Security Department,⁵ repeatedly tried to assure industry that it did not intend to disclose shared information regarding security incidents. Two of the exceptions NIPC frequently cited as possible legitimate exemptions from FOIA were (d) and (g) above regarding commercial confidential information and information compiled for law enforcement purposes, respectively. The “commercial confidential” exception was regarded by many as too vague to be meaningful. The law enforcement exemption, however, was especially plausible because (1) NIPC was located in the nation’s law enforcement department (FBI/DOJ) and its mission, as set forth in Presidential Decision Directive 63 (PDD-63), was to provide “timely warnings of international threats, comprehensive analyses and law enforcement investigation and response.”⁶

Nevertheless, verbal assurances did little to assuage industry fears. Absent a specific exemption, FOIA determinations remained subjective and created an environment of uncertainty that chilled the information sharing atmosphere. Indeed, a review of agency FOIA rules and FOIA litigation quickly reveals discrepancies regarding the protection or disclosure of requested information. In addition to FOIA concerns, there were no legal protections controlling the handling, storage, and use of shared information or restrictions on its disclosure. Industry, therefore, remained skeptical that this information would be protected and many considered the risks associated with sharing information to be greater than the possible benefit of government assistance with security breaches.

Current Situation

Section 214 of the Homeland Security Act was intended to address these concerns. It added an additional FOIA exemption for “critical infrastructure information (including the

identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems....” It also provided statutory protections regarding the receipt, handling, and storage of shared critical infrastructure information. *The Act’s definitions of “critical infrastructure” and “protected systems” are vague, however, and the proposed rule’s lack of explanation or clarification of these definitions undercuts the purpose of Section 214 and injects new uncertainties into the information sharing atmosphere.*

Section 2 of the Act defines “critical infrastructure” as having the same meaning as that used in the USA PATRIOT Act:

“(e) Critical Infrastructure Defined.—In this section, the term “critical infrastructure” means *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 or safety, or any combination of those matters.”⁷

The proposed rule cites the same definition, but does not provide any further elaboration or clarification of the types of “systems and assets” encompassed within this term. The only other statutory reference that provides further elaboration on critical infrastructure is Section 201(d)(5) of the Act, regarding the responsibilities of DHS’s Information Analysis and Infrastructure Protection Directorate (IAIP), which states that the IAIP shall:

“[D]evelop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including power production, generation, and distribution systems, information technology and telecommunications systems (including satellites), electronic financial and property record storage and transmission systems,

emergency preparedness communications systems, and the physical and technological assets that support such systems.”

This provision provides little clarification regarding what the Act considers critical infrastructure because the listing in this section lumps together “key resources” and “critical infrastructure” and includes “physical and technological assets that support such systems.”

Further explanation is needed regarding what systems are considered critical infrastructure. Without such a clarification, the Act’s definition of critical infrastructure is problematic and invites confusion and speculation by both the private sector and courts regarding what systems would be included within its scope. Other official documents do little to define or explain what systems comprise critical infrastructure. Consider the following references to “critical infrastructure”:

- ◆ Presidential Decision Directive-63 (PDD-63) states that: “Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.”⁸
- ◆ Executive Order (EO) 13231 states that: “The protection program authorized by this order shall consist of continuous efforts to secure information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support such systems. Protection of these systems is essential to the telecommunications, energy, financial services, manufacturing, water, transportation, health care, and emergency services.”⁹ On February 28, 2003, Executive Order 13286 amended EO 13231 in its entirety. The amended EO omits the listing of critical industry

sectors and simply states that it is intended “to ensure protection of information systems for critical infrastructure, including emergency preparedness communications and the physical assets that support such systems....” Section 3 of the amended EO 13231 does, however, state that the National Infrastructure Advisory Council (NIAC) “shall provide...advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services.”¹⁰ Thus, *the original EO 13231 added* manufacturing and health care systems to the PDD-63 list, but *the amended EO eliminated* mention of telecommunications (except for emergency preparedness communications), health care, and water systems and referred to “emergency government services” instead of the broader term “emergency services” used in the original EO.

- ♦ *The National Strategy for Homeland Security*, released by the White House on July 16, 2002, lists the critical infrastructure sectors as agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, and postal and shipping.¹¹ Thus, it suddenly expanded the list of critical infrastructures cited in PDD-63 and EO 13231 by adding agriculture, food, public health, government, defense industrial base, information, chemicals and hazardous materials, and postal and shipping systems. It eliminated, however, manufacturing, which was retained in the amended EO 13231.
- ♦ *The National Strategy to Secure Cyberspace*, released by the White House on February 14, 2003, cites the same critical infrastructure sectors as the *Homeland Security Strategy*,¹² as does *The National Strategy for the Physical Protection of Critical*

Infrastructures and Key Assets, released March 4, 2003.¹³ Both of these documents are implementing components of the *Homeland Security Strategy*.¹⁴ *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* offers the most thorough explanation of the components of critical infrastructure that are vulnerable and need protected. This work could serve as a good starting point for developing a detailed explanation, including examples, of the types of systems that would be considered critical infrastructure within the scope of the proposed rule.

It is important to note that the only codified definition for critical infrastructure is the broad definition included in the PATRIOT Act and the Homeland Security Act. The fact that the definition includes “systems and assets, whether physical or virtual” within the definition of critical infrastructure is significant. The *Homeland Security Strategy* carries this concept further by discussing “assets, functions, and systems within each critical infrastructure” as well as “key assets:”

“In addition to our critical infrastructure, our country must also protect a number of key assets—individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation’s morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons.... Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community.”¹⁵

The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets elaborates on the key assets theme, placing them in five categories: (1) national monuments and icons, (2) nuclear power plants, (3) dams, (4) government facilities, and (5)

commercial key assets.¹⁶ It notes that these assets “represent a broad array of unique facilities, sites, and structures whose disruption or destruction could have significant consequences across multiple dimensions.”¹⁷ Some are centers of government and commerce, others “house significant amounts of hazardous materials, fuels, and chemical catalysts that enable important production and processing functions.”¹⁸ Are these key assets now to be considered another category of critical infrastructure? Considering how information technology systems now control almost every aspect of HVAC and environmental systems and sensors as well as facility entry, surveillance, and other means of protecting and securing physical structures, are these systems that support key assets also to be considered within the scope of “systems and assets, whether physical or virtual” protected under the Act’s definition of “critical infrastructure” or “protected systems?”

“Section 214 of the Act defines “protected systems” as:

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component of hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.”

What is protected by the Act in Section 214 is “critical infrastructure information” which is defined by Section 212 as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems....” If it is difficult, however, to discern whether a system is a critical infrastructure or protected system, how is a company to know if information pertaining to their systems will be protected? For example, is a small or medium-

sized enterprise that supplies a critical component to Lockheed Martin covered because Lockheed's systems fall within the defense industrial base? Do *all* of Lockheed's systems qualify for protection or just some of them? What medical systems are covered, if any? Public and private? Executive Order 13231 included "health care," but the February 28, 2003 amendment to the EO eliminated it, and the National Strategies all refer to "public health." Are private sector emergency services included? The original Executive Order 13231 referred to "emergency services," but the amended version lists "emergency government services." What services are included within this category? What about manufacturing systems that were included in both the original and amended EO 13231 but mysteriously dropped from the *National Strategies*? Would key retail systems that could significantly impact national economic security (per the Act's broad definition) be considered as a critical infrastructure or protected systems, even though retail is not one of the enumerated sectors specifically mentioned in official documents?

The statutory definition of "critical infrastructure" and the varying definitions of it within official Administration documents would be confusing enough, but the *Homeland Security Strategy* goes on to note that even if a system *is* a critical infrastructure system, it may not actually be "critical:"

"The assets, functions, and systems within each critical infrastructure sector are not equally important. The transportation sector is vital, but not every bridge is critical to the Nation as a whole. Accordingly, the federal government will apply a consistent methodology to focus its effort on the highest priorities, and the federal budget will differentiate resources required for critical infrastructure protection from resources required for other important protection activities. The federal government will work

closely with state and local governments to develop and apply compatible approaches to ensure protection for critical assets, systems, and functions at all levels of society.”¹⁹

This raises additional questions. Even if a system *is* deemed to be within a critical infrastructure, is shared information regarding that system only protected if the system is “critical to the Nation as a whole” or if it is within an area that the federal government has decided to allocate budget resources to protect, as outlined in the *Homeland Security Strategy*?

A detailed discussion of the types of systems that will be considered critical infrastructure or protected systems, including examples, is critically needed in the rule. *We believe the proposed rule should be modified to more clearly delineate (a) what “systems and assets” are included within the term critical infrastructures, (b) what are types of systems would be considered protected systems, and (c) of these, which are considered “so vital to the United States” that the incapacity or destruction of these systems and assets would have a debilitating impact.* Absent this elaboration, information sharing will continue to be choked by uncertainty regarding FOIA requests and whether the submitted information will be afforded the other statutory protections provided in Section 214, which include:

- ◆ An exemption from ex parte communication rules;
- ◆ A prohibition against its direct use in civil actions;
- ◆ A prohibition against its use or disclosure for any other purpose (except limited exceptions for criminal matters or disclosures to Congress or the Comptroller General);
- ◆ Limitations on sharing it with state or local government; and
- ◆ Protection against waiver of any applicable privilege or protection, such as that associated with trade secrets.

The process of developing a comprehensive explanation (with supporting examples) of the systems deemed to be considered critical infrastructure and protected systems would provide valuable guidance (a) to the CII Program Manager and help ensure consistent determinations as personnel moved in and out of that position, and (b) to courts ruling on challenges to FOIA requests which were denied using the new exemption.

Looking Ahead

The irony is that more information may actually have been protected from FOIA disclosures prior to the enactment of Section 214. Previously, *all* information – irrespective of whether it was critical infrastructure information -- shared with NIPC could possibly have been protected under the commercial confidential and law enforcement exceptions to FOIA. The Act, however, arguably removes the law enforcement exemption because it transferred NIPC from FBI/DOJ to DHS, which does not have law enforcement as an enumerated part of its mission. In fact, Section 101(b)(2) of the Act specifically states that “primary responsibilities for investigating and prosecuting acts of terrorism shall be vested not in the Department, but rather in Federal, State, and local law enforcement agencies with jurisdiction over the acts in question.”

Moreover, the Act limits protection of shared information to that pertaining to critical infrastructure or protected systems, thereby exempting a major groups of systems, including those of home users, service industries, and many small and medium-sized enterprises, any of which could be used to launch an attack against critical infrastructure. In a globally connected network with interdependencies between all types and sizes of systems, the protections for critical infrastructure and protected systems are diminished if only a portion of the systems are covered by the Act. We hope that DHS will keep these considerations in mind when

contemplating future amendments to the Act and will recommend protection for *all* shared information, irrespective of whether it pertains to a critical infrastructure or protected system.

III. To reduce uncertainties, a procedure should be established in the rule to allow companies to receive an advanced determination from DHS regarding whether specific systems qualify as critical infrastructure or protected systems.

Section 29.6 of the proposed rule provides for a presumption of protection for all information submitted according to outlined procedures until such time as the Critical Infrastructure Information Program Manager makes a final decision whether the information is Protected CII. Thus, there is uncertainty both before and after information is shared. *To provide increased incentive for companies to share computer security incident information and to reduce uncertainty, we believe the rule should set forth an easy procedure by which a business could receive an advance determination from the CII Program Manager whether their systems qualified as critical infrastructure or protected systems.* Thus, businesses would be assured when they submitted information that it would be afforded the statutory protections, including an exemption from FOIA requests. An added advantage to this process, is it would encourage interaction between the private sector and the IAIP and CII Program Manager, thereby increasing the likelihood that when the company does encounter a problem, it will contact NIPC or the CII Program Manager.

IV. Even if information is protected as information pertaining to critical infrastructure or protected systems, gaping holes in the protection of this information significantly weaken this protection through its allowed use in criminal investigations and prosecutions and its disclosure to Congress and the GAO without (a) written precautions against further disclosure and (b) notification to the submitting party.

Section 214(a)(1)(D) of the Act and Section 29.8(f) of the rule authorize the use and disclosure of the shared information, without written consent of the submitting entity, to (a) further an investigation or prosecution of a criminal act, or (b) provide information to either

House of Congress or the Comptroller General. Although Section 29.8 of the proposed rule requires written authorization from senior DHS personnel prior to such disclosure, there is no provision in the rule requiring notification to the submitting entity. *Even if the Act does not require consent for such disclosure or use, we believe the rules should include a notice of disclosure to the submitting party.* They could then take steps, if desired, to protect against further disclosure of the information by the receiving entity. For example, the submitting entity could file motions to quash or seek to have the evidence kept under seal. They could also appeal to Congress or the GAO to keep the information confidential.

The use of shared critical infrastructure information in criminal proceedings has always been a fear of industry. Notification would ease this concern and provide greater incentive to share information, whereas no notification leaves the submitting party open to possible repercussions from the disclosure that may be prevented had they been provided notice of disclosure.

Additionally, the proposed rule does not provide for any labeling of the disclosed information that might discourage further disclosure. *We believe a notice visibly attached to the information which informs the receiving entity that the information is Protected CII and advises against further disclosure would help prevent widespread dissemination of the information and would instill greater confidence in the CII Program.*

V. Sharing critical infrastructure information with foreign governments as provided in Sections 29.1(a)(4), 29.1(b), and 29.8(j) of the proposed rule is not authorized by the Act and introduces serious uncertainties into the information sharing atmosphere.

The proposed rule impermissibly provides for Protected CII to be shared with foreign governments. There is no such provision within Section 214. Specific provisions are included within Section 214 of the Act to allow the information to be shared with Federal, state, and local

governments, but it does not allow disclosure to any foreign government or entity. Indeed, the word “foreign” does not even appear in Section 214 of the Act. Moreover, Section 214(f) of the Act imposes criminal penalties on any officer or employee of the U.S. Government who “knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this for improper disclosure of critical infrastructure information....” Therefore, this provision of the rule not only is outside the scope of the Act, it could expose Federal personnel to criminal penalties.

The nature of interconnected networks and packet switching makes it very likely that communications may be routed through foreign countries before reaching their destination. Providing CII information to foreign governments would (1) remove it from the jurisdiction of U.S. jurisdiction, (2) increase uncertainty regarding the protection of shared information, and (3) violate the express provisions of the Act. *We recommend these references to sharing Protected CII with foreign government be stricken from the proposed rule to bring it into conformity with the Act.*

VI. The source of shared information should be more specifically protected in the CII database by encrypting identifying information or using a tracking or identification number assigned to the submitting party.

Section 29.4(e) states that the CII Program Manager “shall develop and use an electronic database, to be known as the “Critical Infrastructure Information Management System” (CIIMS), to record the receipt, acknowledgement, validation, storage, destruction, and disclosure of the Protected CII.” Section 29.6(d)(2) requires the CII Program Manager to include the date of receipt, name of submitter, description of information, an date and manner of acknowledgement in the database. Despite all best efforts, GAO reports are replete with examples of security

breaches of federal information systems. This particular database can be expected to be a target of hackers, theft, or sabotage, and one serious breach could cause significant damage to years of effort and the intention of the Act to facilitate the sharing of security incident information.

Therefore, we suggest that the proposed rule require the name of the submitting entity in the database to be either encrypted or replaced by a tracking or identification number that is assigned to the submitting party.

VII. Although no private right of action is provided by the Act, the rules should establish a procedure for addressing, and potentially investigating, grievances or complaints regarding the manner in which shared information was handled and protected.

Section 215 of the Act specifically precludes any private right of action to enforce any provision of the Act. Although the Act contains no such provision, Section 29.8(f)(2) of the rule authorizes any U.S. Government officer or employee to disclose Protected CII, without the consent of the submitting party, to the DHS Inspector General or any person designated by the Secretary of DHS if they believe the information evidences mismanagement, an abuse of authority, conduct in violation of the Act, etc. The proposed rule does not, however, establish procedures for the submitting party to complain or file a grievance to DHS regarding the receipt, care, and storage of Protected CII.

We believe that a simple complaint/grievance procedure should be included in the rule to (a) enable a better public-private exchange regarding the operations of the CII Program, (b) provide a mechanism for addressing the concerns of submitting parties, and (c) help the CII Program become more user-friendly and trusted.

VIII. Conclusion

SAIC's Enterprise Security Solutions Group is one of the largest information security providers to the federal government. We also have a substantial commercial business and

operate a critical infrastructure ISAC. We believe that the suggestions offered in these comments provide common sense, practical approaches to weaknesses within the proposed rulemaking. Every effort must be made to reduce uncertainty in the information sharing atmosphere and to provide incentives to the private sector to engage and work with the CII Program. Every effort must also be made to make the CII Program user friendly and trustworthy.

By providing a detailed explanation and examples of what types of systems are considered critical infrastructure or protected systems within the scope of the Act and rule, the greatest area of uncertainty and confusion will be addressed. A procedure that would provide companies with an advance determination regarding their systems would provide an incentive to private sector entities to establish a relationship with the CII Program, facilitate information sharing, and eliminate an area of uncertainty. Additional steps to safeguard the identity of the submitting entity, such as using encryption or an identifier number, when entering information in the central database is another easy step toward confidence and certainty. Likewise, if information is to be shared, the courtesy of a notification to the submitting party would help reduce anxieties about disclosure of the information for criminal proceedings, Congressional inquiries, or GAO activities.

It is also important that the CII Program provide a procedure for complaints or grievances to enable the Program Manager to correct problems, address concerns, and maintain a user-friendly atmosphere that is critical to information sharing. Lastly, it is critical that the rule not exceed the legal parameters of the Act, especially regarding disclosure of shared information. In this regard, it is important that rule be amended to remove provisions allowing Protected CII to be shared with foreign governments.

¹ Department of Homeland Security, *Procedures for Handling Critical Infrastructure Information: Notice of Proposed Rulemaking*, 68 Fed. Reg. 18,524 (Apr. 15, 2003); <http://frwebgate1.access.gpo.gov/cgi-bin/waisgate.cgi?WAISdocID=92441410069+0+0+0&WAIAction=retrieve>.

² 6 CFR will be amended by adding Part 29 to accommodate the final rule.

³ A. Marshall Acuff, Jr., “Information Security Impacting Securities Valuations: Information Technology and the Internet Changing the Face of Business,” Salomon Smith Barney, 2000, at 5-6, <http://www.ciao.gov/industry/SummitLibrary/InformationSecurityImpactingSecuritiesValuations.pdf>.

⁴ 5 U.S.C. Section 552(b); <http://www4.law.cornell.edu/uscode/5/552.html>.

⁵ The National Infrastructure Protection Center (except for the Computer Investigations and Operations Section, was moved to the Department of Homeland Security pursuant to Title II, Subtitle A, Section 201(g)(1) of the Homeland Security Act.

⁶ *Presidential Decision Directive/NSC-63: Critical Infrastructure Protection*, May 22, 1998; <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>, (hereinafter “PDD-63”).

⁷ *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act of 2001), Pub. Law 107-56, Section 1016(e) (emphasis added); http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011025_hr3162_usa_patriot_bill.html.

⁸ PDD-63 at 1.

⁹ Executive Order 13231, “Critical Infrastructure Protection in the Information Age, Oct. 16, 2001; <http://www.fas.org/irp/offdocs/eo/eo-13231.htm>.

¹⁰ Executive Order 13286, “Amendment of Executive Orders, and Other Actions, in Connection With the Transfer of Certain Functions to the Secretary of Homeland Security,” Section 7, Feb. 28, 2003; <http://www.fas.org/irp/offdocs/eo/eo-13286.htm>.

¹¹ *The National Strategy for Homeland Security*, “Protecting Critical Infrastructures and Key Assets,” July 16, 2002 at 30, 32; <http://www.whitehouse.gov/homeland/book/index.html>.

¹² *The National Strategy to Secure Cyberspace*, Feb. 14, 2003, at 4; http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

¹³ *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets*, Mar. 4, 2003 at 35; http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf.

¹⁴ *The National Strategy for Cyberspace Security* at 1.

¹⁵ *The National Strategy for Homeland Security* at 30.

¹⁶ *The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets* at 71-80.

¹⁷ *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* at 71.

¹⁸ *Id.*

¹⁹ *The National Strategy for Homeland Security* at 30.