DEPARTMENT OF HOMELAND SECURITY

Office of the Secretary

6 CFR Part 29

RIN 1601–AA14

Procedures for Handling Critical Infrastructure Information; Interim Rule

AGENCY: Office of the Secretary, Department of Homeland Security.

ACTION: Interim rule with request for comments.

SUMMARY: This interim rule establishes procedures to implement section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of critical infrastructure information voluntarily submitted to the Department of Homeland Security. The protection of critical infrastructure reduces the vulnerability of the United States to acts of terrorism. The purpose of this regulation is to encourage private sector entities to share information pertaining to their particular and unique vulnerabilities, as well as those that may be systemic and sector-wide. As part of its responsibilities under the Homeland Security Act of 2002, this information will be analyzed by the Department of Homeland Security to develop a more thorough understanding of the critical infrastructure vulnerabilities of the nation. By offering an opportunity for protection from disclosure under the Freedom of Information Act for information that qualifies under section 214, the Department will assure private sector entities that their information will be safeguarded from abuse by competitors or the open market. In addition, information from individual private sector entities combined with those from other entities, will create a broad perspective from which the Federal government, State and local governments, and individual entities and organizations in the private sector can gain a better understanding of how to design and develop structures and improvements to strengthen and defend those infrastructure vulnerabilities from future attacks.

DATES: This interim rule is effective February 20, 2004. Comments and related material must reach the Department of Homeland Security on or before May 20, 2004.

ADDRESSES: Submit written comments to Janice Pesyna, Office of the General Counsel, Department of Homeland Security, Washington, DC 20528. Electronic comments may be submitted to *cii.regcomments@DHS.gov*.

FOR FURTHER INFORMATION CONTACT: Janice Pesyna, Office of the General Counsel, (202) 205–4857, or Fred Herr, Information Analysis and Infrastructure Protection Directorate, (202) 360–3023, not a toll-free call.

SUPPLEMENTARY INFORMATION:

Public Participation and New Request for Comments

The Department of Homeland Security (Department or DHS) encourages the public to participate in this rulemaking by submitting comments and related materials. All comments received will be posted, without change, to the DHS Web site (*http://www.dhs.gov/pcii/*) and will include any personal information provided.

Submitting comments: To submit a comment, please include the full name and address of the person submitting the comment, identify the docket number for this rulemaking, indicate the specific section of this document to which each comment applies, and give the reason for each comment. Comments and supporting material may be submitted by electronic means, mail, or delivery to the Department of Homeland Security, Washington, DC 20328. The Department will consider all comments and material received during the comment period. The Department may change this rule in view of them.

Regulatory History

On April 15, 2003, the Department published a notice of proposed rulemaking entitled ''Procedures for Handling Critical Infrastructure Information'' in the **Federal Register** (68 FR 18523), 6 CFR part 29, RIN 1601–AA14. As stated in the notice of proposed rulemaking, the Department intended to implement this interim rule as soon as possible. The Department finds that the need to receive critical infrastructure information, as soon as practicable, furnishes good cause for this interim rule to take effect immediately under section 808 of the Congressional Review Act.

For many years, private industry has indicated that its reluctance to share critical infrastructure information with the Federal government is based upon a concern that the information will not be adequately protected from disclosure to the public. Furthermore, private sector entities fear that entities intending to harm our nation, as well as potential business competitors, could seek to use the Freedom of Information Act or other disclosure processes to obtain sensitive or confidential business information not otherwise available to the public. Release of such information could facilitate the efforts of those persons or entities planning or attempting to cause physical or economic harm to our nation or to a particular company or industry.

The responsibilities of the Department include taking action to prevent terrorist attacks within the United States and reducing the vulnerability of the United States to acts of terrorism. The reduction of that vulnerability includes the protection of vital physical or computer-based systems and assets, collectively referred to as ''critical infrastructure,'' the incapacitation or destruction of which would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of these matters.

The Department recognizes the importance of receiving information from those with direct knowledge of the security of that critical infrastructure in order to help reduce our nation's vulnerability to acts of terrorism. The Department believes the voluntary sharing of critical infrastructure information (CII) has been slowed due to concerns that information might be released to the public.

The Department recognizes that its receipt of information pertaining to the security of critical infrastructure, which is not customarily within the public domain, is best encouraged through the assurance that such information will be utilized for securing the United States and will not be disseminated to the general public. Accordingly, section 214 of the Homeland Security Act, subtitle B of title 2, which is referenced as the Critical Infrastructure Information Act of 2002 (CII Act of 2002), directly addressed this problem by establishing a program that protects from disclosure to the general public any CII that is voluntarily provided to the Department. Section 214(f) of the statute provides for fines and imprisonment under title 18 (Crimes and Criminal Procedure) of the United States Code for unauthorized disclosure of CII.

The interim rule will provide the Department with the framework necessary to receive CII and protect it from disclosure to the general public. This interim rule provides flexibility to allow the Department to adapt as program operations evolve. This interim rule sets out a basic set of regulations that implements the Protected CII Program. The Department will continue to consider public comments to this interim rule and determine whether possible supplemental regulations are needed as experience is gained with implementing the CII Act of 2002.

Discussion of Comments and Changes

The Department received 117 different sets of comments on the proposed rule during the initial comment period. The Department has considered all of these 117 sets of comments, and summaries of the comments and the Department's responses follow.

CII and Protected CII

The Department received six comments suggesting the need to make the distinction between CII and Protected CII clearer throughout the rule. This regulation establishes the program for the receipt, handling, use, and storage of a specialized category of information that is voluntarily submitted to the Department and meets the criteria for Protected CII. Not all CII necessarily will be Protected CII. Recognizing that the proposed rule did not in all instances use the terms ''CII'' and ''Protected CII'' consistently, the interim rule has been modified throughout where appropriate.

Indirect Submissions

The Department received 20 comments expressing concern regarding the proposed provision that would enable other Federal government entities to act as conduits for submissions of CII to the Department. Comments observed that extending the protections of the CII Act of 2002 to information submitted to agencies other than the Department was outside the authority of the Department. Further, comments highlighted the increased potential for unauthorized use and disclosure of information, as well as the burden that indirect submissions might place on other entities. Comments requested that all references to indirect submissions be removed and that the rule's terms be clarified so that no section could be interpreted to express or imply that material may be submitted to another Federal government agency.

Three comments supported allowing indirect submissions as proposed in the notice of proposed rulemaking; however, these comments, too, highlighted the need for clarification of how such a provision might be implemented and sought additional clarification to ensure that questions regarding the status of CII submitted to an entity other than the Department will be avoided. Support for indirect submissions recognized the Department's original intent, which was to further encourage the sharing of CII with the Federal government. Owners and operators of the nation's critical infrastructures have established relationships with other Federal agencies (*e.g.*, agencies that are sector leads for a particular infrastructure) and are comfortable sharing information with those entities. The Department did not want to impede information sharing and, consequently, our ability to protect our nation, by limiting the ability of submitters to share CII with the Department using those existing relationships.

Recognizing that, at this time, implementation of such a provision would present not only operational but, more importantly, also significant program oversight challenges, the Department has removed references throughout the rule to indirect submissions. Specifically, § 29.1 has been revised to ensure that ''receive'' is not interpreted to mean that material may be submitted to Federal government entities other than the Department. Section 29.2(i) has been revised to clarify that only the Department and no other Federal government entity shall be the recipient of voluntarily submitted CII. Sections 29.5(a), 29.5(b), and 29.5(c) have been revised to remove references to indirect submissions and to clarify that submissions must be made directly to the Protected CII Program Manager or the Program Manager's designee.

After the Protected CII Program has become operational, however, and pending additional legal and related analyses, the Department anticipates the development of appropriate mechanisms to allow for indirect submissions in the final rule and would welcome comments on appropriate procedures for the implementation of indirect submissions. Comments in support of, or opposed to, the proposed framework for indirect submission of CII to DHS should fully set forth, with relevant citations to the CII Act of 2002 and any other statutory, legislative, or case authorities that may be applicable, the basis for the position they advance.

Relationship Between Protected CII and Other Similar Regulations

The Department received four comments regarding the relationship between this rule and similar Federal agency rules such as the Transportation Security Administration's (TSA) Sensitive Security Information (SSI) rule and the Federal Energy Regulatory Commission's (FERC) Critical Energy Infrastructure Information (CEII) rule. The comments requested that the Department review and clarify the relation of the Department's procedures with similar procedures created by other Federal agencies for the same types of data.

Under certain limited circumstances, there may be information designated as CII under this interim rule that may also constitute SSI under regulations administered by TSA. SSI is information that the Administrator of TSA has determined must be protected from unauthorized disclosure in order to ensure transportation security. The TSA Administrator's authority to designate information as SSI is derived from 49 U.S.C. 114(s).

TSA's regulation implementing this authority, which is set forth at 49 CFR part 1520, specifies certain categories of information that are subject to restrictions on disclosure, both in the hands of certain regulated parties and in the hands of Federal agencies. Currently, the SSI regulation applies primarily to security information related to the aviation sector such as: Security programs and procedures of airport and aircraft operators; procedures TSA uses to perform security screening of airline passengers and baggage; and information detailing vulnerabilities in the aviation system or a facility. SSI is created by airports and aircraft operators and other regulated parties, pursuant to regulatory requirements. TSA also creates SSI, such as screening procedures and certain non-public security directives it issues to regulated parties. The SSI regulation prohibits regulated parties from disseminating SSI, except to those employees, contractors, or agents who have a need to know the information in order to carry out security duties.

Like the provisions of the Homeland Security Act governing CII, TSA's SSI statute and its implementing regulation trigger one of the statutory exemptions to the general disclosure requirements of the Freedom of Information Act (FOIA). *See* 5 U.S.C. 552(b)(3). Thus, both Protected CII and SSI held by the Federal government are exempt from public disclosure under the FOIA. In addition, TSA is currently considering amendments to its SSI regulation that would make it civilly enforceable against employees of DHS and the Department of Transportation, which are the Federal agencies most likely to maintain SSI. In contrast, unauthorized disclosure of Protected CII by a Federal employee is subject to criminal penalties.

Another key difference between SSI and Protected CII is the extent to which a Federal employee may disclose such information. Under TSA's SSI regulation, TSA may disclose SSI to persons with a need to know in order to carry out transportation security duties. This includes persons both within and outside the Federal

government. This rule proposes disclosure of Protected CII to entities that have entered into express written agreements with the Department and, in some cases, requires the written consent of the submitter before disclosure is permitted. Thus, in cases where information qualifies as both SSI and Protected CII, a Federal employee must treat the information according to the stricter disclosure limitations applicable to Protected CII.

In practice, the situations in which information constitutes both SSI and Protected CII may be limited. For the most part, information that is SSI is created by TSA or is required to be submitted to TSA or to another part of the Federal government. Therefore, it ordinarily will not be voluntarily submitted, which is a required element for Protected CII designation. In addition, SSI might or might not relate to critical infrastructure assets. Nonetheless, DHS will work to ensure that TSA's SSI regulation identifies any instances in which there may be an overlap between the SSI and Protected CII regulatory schemes and clarifies the applicable requirements for the handling of such information.

Other comments expressed concern regarding the relationship between Protected CII and the rule set forth in the Critical Energy Infrastructure Information program of the Federal Energy Regulatory Commission. These rules are not the same. They operate in a very different fashion with respect to the disclosure requirements of FOIA. On February 21, 2003, FERC promulgated final regulations establishing the CEII procedures, whereby persons with a demonstrated need to know who agree to no further dissemination can be provided with certain information not otherwise available through FOIA. (68 FR 9857 (March 3, 2003)) While information that meets the FERC definition of CEII remains protected from disclosure under existing FOIA exemptions, an alternative means of sharing certain CEII is established, including through a CEII Coordinator charged with verification of the need of requesters for access and the use of non-disclosure agreements via a non-FOIA disclosure track. In other words, the FERC program does not create any exempting authority that would change FOIA disclosure requirements, whereas section 214 of the Homeland Security Act, which is the basis for the Department's CII regulations, does.

Definitions

The Department received several comments regarding terms defined in § 29.2. The following sections address each of the terms in greater detail.

Critical Infrastructure and Protected System

The Department received two comments expressing concern that the terms ''critical infrastructure'' and ''protected system'' were not sufficiently defined. The comments suggested that examples be provided and that phrases such as ''debilitating impact'' be further defined. The Department notes that Congress in the CII Act of 2002 prescribed the definition of ''protected system.'' The Department believes that the definition provides an appropriate degree of flexibility necessary to ensure that information pertaining to the protection of these assets could potentially be shared with the Department.

That said, the Department bases its construction of the regulatory definition on the CII Act of 2002 itself. The Department is mindful that private sector submitters, as the owners and operators of most of the nation's critical infrastructures, are the most well versed as to what information in their particular sector or industry might qualify as CII; therefore, the Department does not wish to unduly restrict the scope of what may be submitted as CII under the Act. As part of its evaluation process in determining whether information meets the criteria for Protected CII, the Department will consider the belief of the submitter that the information merits protection under the Act.

Critical Infrastructure Information

The Department received 11 comments suggesting that the definition of CII be expanded and clarified. Several of the comments wished to expand the definition to include network and topology information for critical infrastructures. The comments also emphasized that expansion of the definition would provide submitters with guidance regarding the type of information that the Department is looking to receive and also ensure that other important information is afforded the protections of the CII Act of 2002, therefore further encouraging submissions. The comments requested that a detailed explanation of ''not customarily in the public domain'' be provided and encouraged the Department to develop procedures for evaluating whether information is in the public domain. One comment requested that the rule further describe the specific records or information that would be considered by the Department for protection under the CII Act of 2002. Further, comments suggested that the rule specify what information is not CII so that submitters know what types of information should not be submitted. The Department notes that Congress in the CII Act of 2002 prescribed the definition of CII.

The Department believes that the definition provides the appropriate degree of flexibility necessary to further promote information sharing by providing submitters with an opportunity to provide the information they believe meets the definition and should be protected.

The Department also received two comments noting that the proposed rule defined CII as both records and information. Comments suggested that the term ''record'' be removed from the rule while other comments supported defining CII as both. As a practical matter, these two terms are virtually interchangeable in a context such as this. Accordingly, § 29.2 has been revised to say ''CII consists of records including and information concerning * * *''

Voluntary/Voluntarily

The Department received 11 comments regarding the broad definition of ''voluntary.'' The rule defines information that is not voluntarily provided as that information which the Department has exercised legal authority to obtain. The comments expressed concern that this could permit submitters to share with the Department information that is involuntarily collected by other Federal entities. The rule follows the explicit language of the Homeland Security Act and allows for the voluntary submission of information to the Department that is involuntarily collected by other Federal agencies, subject to certain requirements. These restrictions are found throughout the rule, primarily in § 29.3(a), which states that its procedures do not apply to or affect any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted pursuant to the CII Act of 2002), and § 29.5(a)(4), which has been added to the rule to address specific concerns raised by commenters. Section 29.5(a)(4) requires submitters to certify that the particular information is being voluntarily provided to the Department; that the information is not being submitted in lieu of independent compliance with a Federal legal requirement; that the information is of a type not customarily in the public domain; and whether the information is required to be submitted to a Federal

agency. If the information is required to be submitted to a Federal agency, the submitter must identify the Federal agency and the legal authority mandating that submission.

Good Faith

The Department received 26 comments requesting that the rule define the term ''good faith'' and establish procedures for determining that material has been submitted in good faith. Comments also asserted that the proposed rule had the potential to establish a system where material that was not submitted in good faith, and thus does not qualify for protection, would never be made public. Comments suggested that the Protected CII Program Manager should inform submitters when a decision is made that information was not submitted in good faith and provide them with an opportunity to provide an explanation. Other comments recommended deleting references to ''good faith'' in their entirety.

The Protected CII program is based upon a relationship of trust with the public that the information submitted will be carefully evaluated, marked, and utilized for the purposes of protecting the nation. As recommended by a number of these comments, § 29.5 has been revised, deleting the requirement for the submitters to *certify* that they are submitting the information in good faith. Instead, § 29.5 now provides that the submitters are presumed to have submitted the information in good faith. False representations may constitute a violation of 18 U.S.C. 1001 and are punishable by fines and imprisonment. The intent of such a provision is to provide a remedy to prevent a party from repetitively submitting information in bad faith solely to consume agency resources and from submitting information in an attempt to shield from the public any evidence of wrongdoing.

Independently Obtained Information

The Department received five comments regarding the definition of ''independently obtained information.'' Comments claimed that the proposed definition was not consistent with the CII Act of 2002. In addition, one comment correctly noted that to ensure clarity the provision should be revised to indicate that independently obtained information does not include information that has been directly or indirectly derived from Protected CII. The Department has revised § 29.3(d) to alleviate confusion and ensure consistency with the legislation.

Protected CII Program Management and Administration

Consistent with the CII Act of 2002 and this regulation, the Under Secretary for Information Analysis and Infrastructure Protection (IAIP) is the official responsible for the receipt, safeguarding, storage, handling, and dissemination of Protected CII. The Under Secretary oversees and administers the Protected CII Program. Many comments expressed concern regarding details of the procedural implementation of the Protected CII Program. In addition, other comments recommended that the program begin operations as soon as possible after publication of this interim rule.

To implement this regulation in an efficient manner, the Department intends to use a phased approach that gradually expands the capabilities of the Program to receive submissions. Initially, submissions will be received only by the Protected CII Program Office within the Information Analysis and Infrastructure Directorate (IAIP) of the Department.

Subsequent phases will expand the points of entry for information within the Department. During the initial phase, only paper or electronic submissions (*e.g.,* floppy disks, CDs, etc.) delivered via U.S. Mail, commercial delivery service, courier, facsimile, or hand delivery will be accepted. As the Program evolves, e-mail and oral submissions (*i.e.,* voice mail or person-to-person) will be accepted. The capabilities of the Program to share information that has been validated as Protected CII also will expand. The Department envisions that Federal, State, and local government entities that would like to access and use Protected CII shall enter into an express written agreement with the Department. Such an agreement will outline the responsibilities for handling, using, storing, safeguarding, and disseminating Protected CII; require entities to put in place similar procedures for investigating suspected or actual violations of Protected CII procedures; and establish guidelines for imposing penalty provisions for unauthorized disclosure similar to those identified in the CII Act of 2002 and this regulation. Entities that do not sign such an agreement with the Department will not have access to Protected CII. Initially, the Department intends to share Protected CII only within the IAIP Directorate and with other DHS components, although exceptions may be made on a case-by-case basis. As the Program evolves and agreements with additional entities are finalized, the disclosure of information will expand to other Federal government entities, State, and local government entities, and eventually to foreign governments.

The Department received one comment suggesting that the proposed rule would overburden the Department by creating a situation where only one employee of the Department is responsible for receiving submissions and validating Protected CII. Other comments questioned how the Protected CII Program Manager would have the expertise, resources, and ability to handle the workload that may result from these provisions. The Department does not envision a situation in which only one employee is handling submissions and validating Protected CII. The Under Secretary for IAIP is responsible for directing the Protected CII Program and overseeing its day-to-day operations. In this capacity, the Under Secretary will ensure that the Program Manager or Program Manager's designees consult with other Department officials, as appropriate and necessary, to evaluate the validity of submissions. In addition, a staff and other resources required to perform the responsibilities outlined in the interim rule will support the Protected CII Program Manager. References throughout the rule to the Protected CII Program Manager have been revised to include ''or designees'', where appropriate, to indicate that other individuals will be designated to handle receipt, validation, and other duties related to the day-to-day operations of the Protected CII Program.

The Department also received three comments requesting that the rule be clarified to specify in greater detail the selection, training, and support of Protected CII Officers. The Department intends to encourage Federal, State, and local (including tribal) government entities that have signed an agreement with the Department to access and use Protected CII to appoint a Protected CII Officer who has been trained and is familiar with procedures for safeguarding, handling, transmitting, and using Protected CII. While this is addressed in greater detail in Protected CII Program procedures, the role of Protected CII Officer may be assigned to an individual in addition to their other duties. The Protected CII Program Manager shall establish procedures outlining the responsibilities of Protected CII Officers and will work with Federal government, and State and local entities in the identification, selection, training, and oversight of Protected CII Officers.

The Department received one comment recommending that

implementing directives discussing how the Protected CII Program will be managed be subject to public review and comment. The Department will follow all provisions of the Administrative Procedure Act in implementing the CII Act of 2002 and this regulation; all policies, and changes to policies, that are required to proceed by way of public notice will do so. Program office development, including but not limited to the Protected Critical Infrastructure Information Management System, used for tracking information voluntarily submitted under the Act, will be consistent with the existing standards of the Department and the Federal government. The Department intends to measure and assess the Program's performance and conduct internal audits to ensure that its goals and objectives are met. The Department recognizes that the success of the Protected CII Program depends on submitters and those with whom Protected CII is shared having an understanding and appreciation of Protected CII Program procedures.

Protected CII Management System

The Department received five comments expressing concerns about the Department's ability to adequately ensure the security of the Protected CII Management Systems (PCIIMS) database. The PCIIMS is a tracking system, not a storage database for the PCII itself. The PCIIMS will be used to track the receipt, acknowledgement, validation, storage, dissemination, and disposition of Protected CII. It is the Department's intent that Protected CII will be maintained in a manner that ensures that it is kept separate from information pertaining to the source of the submission. The Department received two comments requesting that the tracking number be extended to material that has been validated as Protected CII. In addition, one comment recommended that there be a mechanism to track the status of material marked as Protected CII in the event that the status of the information changes. The Department has reviewed this regulation and, consistent with this regulation and these comments, the tracking number assigned to the submission will accompany the material from the time that it is received by the Protected CII Program Manager. The Protected CII Program Manager will establish programs and procedures regarding the security of all Protected CII, including the data stored on the Protected CII Management System (PCIIMS). In addition, the Department will ensure compliance with all appropriate Departmental and Federal government information security policies.

Presumption of Protection

The Department received five comments regarding the presumption of protection afforded to submissions received by the Protected CII Program Manager but for which a final validation determination has not been made. These comments asserted that material does not qualify for protection just because it has been submitted to and received by the Department. The Department also received eight comments encouraging the Department to consider including a time frame for making validation determinations. Comments expressed concern that, combined with the presumption of protection, the lack of a time frame for validating submissions could result in material that does not qualify for protection retaining protection for long periods of time. The Department also received four comments supporting the presumption of protection. These comments noted that absent such a provision submitters would be unlikely to submit CII of a sensitive nature. The Department agrees that in order to promote information sharing the presumption of protection is a necessary provision. The Department agrees that the validation of submitted material must be completed in a timely manner. Submitters, the public, and users of Protected CII within Federal, State, local, and foreign governments must be assured that decisions will be made in a timely manner that allows Protected CII to be used appropriately. Additional language has been added to § 29.6(e)(1), therefore, indicating that the Protected CII Program Manager or designees will review and make a validation determination as soon as practicable following receipt of the submission. The Department considered identifying a more specific time frame; however, the Department does not believe it wise to limit the Program Manager's ability to determine what time frame is feasible given the constraints of program resources and the nature of the submissions received.

The Department also agreed with one of the comments that suggested the proposed language should be revised to read ''presumed to be *and* will be treated'' (emphasis added for clarification) in § 29.6(b). Section 29.6(b) has been revised accordingly.

Freedom of Information Act Requests

The Department received nine comments requesting that the rule be clarified to explain how FOIA requests will be handled during the period of time in which the Protected CII Program Manager is making a determination regarding whether the submission is Protected CII. Comments further recommended that when a FOIA request is received, the Protected CII status should be reviewed to ensure that the designation remains appropriate. Further, comments requested that submitters be notified when the Department receives a FOIA request concerning the information that they submitted. FOIA requests concerning Protected CII will be handled in accordance with the Department's existing FOIA processes and Executive Order 12600. *See* U.S. Department of Justice, Office of Information and Privacy's Freedom of Information Act Guide & Privacy Act Overview, May 2002 Edition. The Protected CII Program Manager or designees will work closely with the Department's FOIA Officer to handle FOIA requests of Protected CII in a manner consistent with FOIA.

Marking of Information

The Department received two comments highlighting a potential area of confusion regarding marking of materials for protection under the CII Act of 2002. The comments incorrectly asserted that material would be marked with the ''express statement'' and that the marking would provide direction for the material's handling. It is correct that submitters must include the express statement as identified in § 29.5(a)(3) when material is submitted to the Department; however, that statement is not used in the marking of Protected CII. When such information is validated and has been found to warrant protection under the CII Act of 2002, the Protected CII Program Manager will mark the material with the marking found in § 29.6(c), which makes specific reference to this regulation.

The Department received six comments requesting that the Department include provisions for segregating information so that information that is not protected under the CII Act of 2002 is clearly marked and only information that is absolutely necessary to the protection of the nation's critical infrastructure is kept from public view. The Department does not at this time intend to ''portion mark'' Protected CII. It is the Department's belief that requiring submitters to ''portion mark'' material at the time of submission may impede the full disclosure of information. Instead, the Department will consider a submission to be Protected CII as long as it in substance meets all of the requirements for protection. In making validation determinations, the Department will carefully review the

submitted information against the certification by the submitter to ensure that the information is provided voluntarily, in good faith, and is not required by law to be submitted to DHS.

Storage of Protected CII

The Department received seven comments regarding the storage of Protected CII material. Comments expressed concern that the requirements are not sufficient to protect against unauthorized access. For example, the comments noted that a ''locked desk'' is not generally recognized as a ''secure container.'' In addition, comments suggested that additional safeguards should be considered for information that is aggregated within one facility, area, or system.

In response, § 29.7(b) has been revised to address these concerns about safeguarding Protected CII. In accordance with Federal government requirements for protecting information and information systems, the Department will take proper precautions to ensure that Protected CII is appropriately safeguarded. Furthermore, this section has been revised to clarify how Protected CII should be safeguarded when in the physical possession of a person.

Transmission of Information

The Department received eight comments regarding the treatment of U.S. first class, express, certified, or registered mail and secure electronic means as equivalent means of transmission in terms of the security they provide. Further, comments noted that § 29.7(e) did not allow for use of commercial delivery firms or person-to-person delivery. The comments noted that the proposed rule's specific listing of modes that were acceptable for transmitting information was restrictive. In response, the Department has broadened the language to include any secure means of delivery as determined by the Protected CII Program Manager. This change alleviates any problem of the rule implicitly, but unintentionally, prohibiting other transmission modes that were not included in the list. As technology advances, this language will allow the Department to utilize new transmission modes, as appropriate.

Disclosure of Information

The Department received two comments recommending that any advisories, alerts, and warnings issued to the public should not disclose the source of any voluntarily submitted CII that forms the basis for the warning or information that is proprietary, business sensitive, relates to the submitting person or entity, or is otherwise not appropriately within the public domain. The Department agrees with these comments in significant part. Section 29.8(a) has been modified to include language similar to that contained in the comments.

Twelve comments were received requesting that notification be made to submitters prior to disclosure of their information. Some of the comments also went so far as to request that the prior written consent of the submitter be obtained before Protected CII is disclosed. The comments also suggested that submitters should be made aware of the content of any alerts, advisories, and/or warnings that are issued based on Protected CII. The Department envisions that it will be able to track the disclosure of Protected CII to other Federal government entities and State, and local government entities. In addition, these entities will be asked to track further disclosure of Protected CII within their respective entities. The Department recognizes the desire of submitters to control the release of the information that they submitted; however, such a provision for prior notification has the potential to place a significant administrative burden on the Department. The Department does agree that further disclosure of information beyond those entities or individuals that have entered into a formal agreement with the Department may require the permission of the submitter.

The Department received seven comments regarding disclosure of Protected CII to contractors, each of which encouraged the Department to require contractors to comply with the requirements of this regulation through express written agreements with contractors. The Department received one comment requesting clarification regarding whether State and local governments would be able to share Protected CII with contractors acting on behalf of the Federal government and managing critical infrastructure assets without the submitter authorizing State and local entities to do so. The Department agrees that contractors should be required to comply with the requirements of this regulation. It is the intent of the Department that the Department as well as other Federal, State, and local government entities that access Protected CII shall put in place the necessary written agreements to ensure that the regulations are appropriately adhered to.

The Department received 14 comments regarding the sharing of Protected CII with foreign governments. The comments expressed concern that the CII Act of 2002 did not authorize the Department to share Protected CII with such entities; that express agreements to share Protected CII with foreign governments may be beyond the scope of the Act; and, if sharing information with foreign governments is not beyond the scope of the Act, then senior Department officials, as appropriate, should coordinate the agreements. Comments also questioned how the Department would verify that foreign governments are handling Protected CII appropriately and enforce criminal and administrative penalties if the material is not being handled in a manner consistent with the CII Act of 2002 and this rule. The Department believes that through the establishment of formal agreements with foreign governments, Protected CII can safely and properly be shared for important homeland security purposes. The comments also expressed concern that the proposed rule would allow release of information concerning the source of the Protected CII and other proprietary, business-sensitive information to foreign governments. Accordingly, § 29.8(j) has been revised to address this latter concern by protecting from public disclosure the source of any voluntarily submitted CII that forms the basis for the warning, as well as any information that is proprietary or business sensitive, relates specifically to the submitting party or entity, or is otherwise not appropriate for such disclosure.

Oral Submissions

The Department received one comment expressing concern that oral submission of CII may be chilled by the lack of clarity in the rule concerning the status of notes regarding CII submissions. The comment recommended that the definition of CII be expanded to include notes of oral conversations. The Department intends that notes made by the Protected CII Program Manager or designees shall be presumed to be and will be treated as Protected CII until a validation determination regarding the oral submission and the written version of the oral submission is made otherwise.

The Department received one comment requesting clarification of the process regarding acknowledgement of the receipt of orally submitted CII for protection under the CII Act of 2002. Section 29.6(d) has been revised to explain this process further. In addition, two comments correctly noted that § 29.6(d) was incorrectly numbered in the proposed rule, and the interim rule has been revised accordingly.

Destruction of Information

The Department received three comments noting that the proposed rule used a variety of terms (*e.g.*, ''destroy,'' ''dispose,'' ''disposed,'' and ''disposal of'') to deal with the treatment of material that has been found not to warrant protection. The comments recommended the consistent use of either ''destroy'' or ''destroyed'' throughout the rule in accordance with the Federal Records Act. The interim rule has been revised throughout as appropriate.

Retaining Information for Law Enforcement and/or National Security Reasons

The Department received four comments requesting that the Department clarify what information would be retained for law enforcement and/or national security reasons that would not be Protected CII. The comments requested that language be included to demonstrate that the information would also be protected from disclosure under FOIA. Further, comments recommended that submitters be notified when a submission is retained for such purposes. The Department will retain information for law enforcement and/or national security reasons on a case-by-case basis. In some instances, information that has been found not to warrant protection under the CII Act of 2002 may be of significance for law enforcement and/or national security purposes. In that case, if the information is exempt from disclosure under other FOIA exemptions, the Department will consider such exemptions at the time that a FOIA request is received. In any case, the Department will handle such information in a manner commensurate with its nature and sensitivity.

Deference

The Department received seven comments regarding the deference given to submitters in the Department determination of what is CII. Comments stated that the language is ambiguous and provides too much discretion to the submitter. The Department will evaluate the submitter's claims that information meets the requirements for protection under the CII Act of 2002 and make the final determination regarding whether submitted information meets the requirements for protection. In response to these comments, the Department has removed references to deference. In addition, the Department agreed with two comments suggesting that submitters sign a statement attesting to the validity of their claims that a submission meets the requirements for protection. The Department has added to this interim rule (§ 29.5(a)(4)) the requirement that submitters sign a statement certifying that the submission meets the requirements for protection (*i.e.*, that the information is being provided voluntarily for the purposes of the CII Act of 2002; that the information is not being submitted in lieu of independent compliance with a Federal legal requirement; whether the information is required to be submitted to a Federal agency; and that the information is not customarily in the public domain). It is the intent of this provision to discourage unjustified claims for protection.

Change of Protected CII Status

The Department received 15 comments regarding the change of status from Protected CII to non-Protected CII. The comments recommended that the Protected CII Program Manager notify the submitter and any other parties with whom Protected CII has been shared of any changes in status. The comments also suggested that the circumstances under which a change of status may take place be enumerated in the rule. In response to these comments, § 29.6(f) has been modified to allow the submitter to request in writing that the status of Protected CII material be changed. In addition, the Department recognizes that there may be other circumstances that require the status of Protected CII to be changed. For example, changes may take place if the Program Manager subsequently determines that the information was customarily in the public domain, was required by Federal law or regulation to be submitted to DHS, or is now publicly available through legal means. In addition, § 29.6(f) has been revised to ensure that submitters and those entities with which the Protected CII was shared are made aware of the change in status.

Return and Withdrawal of Material

The Department received seven comments recommending that in addition to maintaining the information without protection and destruction of the information, submitters should be able to indicate that they would like submitted material returned to them in the event that a final validation determination is made that the submission is not Protected CII. Although the Department understands the desire of submitters to retain control over the information that they submitted, including such a provision has the potential to place a significant administrative burden on the Department.

The Department also received one comment requesting that the submitter be provided with the opportunity to withdraw the submission prior to a final validation determination. The Department agrees with this comment and has added language to § 29.6(e)(2)(i)(C) giving submitters an opportunity to withdraw submissions prior to a final validation determination.

Investigation of Violations

The Department received one comment requesting that submitters be notified when an investigation of improper disclosure has begun and the outcome of that investigation, therefore allowing the submitter to take steps to protect information in the event that the material was disclosed improperly. Two additional comments requested that a specific time frame for notification be identified in the rule. The Department disagrees that submitters should be notified when an investigation has begun. It is the Department's belief that at such a time submitters will want to know specific details regarding the suspected or actual violation. The Department will not have specifics until such time as the investigation is concluded and formal findings have been identified.

In addition, one comment was received regarding the requirement that ''all persons authorized to have access to Protected CII'' report suspected or actual violations. The comment suggested that all officers, employees, contractors, and subcontractors of the Department whether authorized to access Protected CII or not should report suspected or actual violations. The Department does not agree with this suggestion. The intent of § 29.9(a) is to encourage those individuals with access to Protected CII to self-report suspected or actual incidents. In addition, individuals that have not been granted access to Protected CII are unlikely to knowingly witness any abuses of Protected CII procedures. Those authorized to access Protected CII will be uniquely qualified to detect suspected or actual incidents of unauthorized access or misuse.

Whistleblower Protection

The Department received 10 comments suggesting that the application of the Whistleblower Protection Act is not sufficient to protect whistleblowers. The comments expressed concern that whistleblowers could be unfairly treated and subject to termination, fines, and imprisonment. This would discourage the accurate reporting of information vital to the public. The Department has modified

§ 29.8(f)(ii) to reference the Whistleblower Protection Act (WPA). Since the Department's intention is to afford the protections of the WPA, by referencing the WPA itself, the Department believes that it clearly ensures the full range of protections offered under the WPA.

An Appeals Process

The Department received two comments requesting that procedures for appealing determinations regarding Protected CII be included in these regulations. One comment suggested that submitters be provided with additional time to justify their assertion that a submission meets the requirements for protection if the submitter makes such a request. The Department believes that the procedures outlined in § 29.6(e) regarding validation determinations provide submitters with adequate time to justify their submissions. If the Department were to allow appeals of validation determinations or permit submitters to take longer than the thirty calendar days to respond, the Department would be contributing to situations in which information that might not be Protected CII remains in protected status.

No Private Right of Action

The Department received one comment concerning the ambiguity introduced by the proposed rule's reference to ''no private rights or privileges'' in § 29.3(e). The Department agreed with this comment and has revised the interim rule to ensure that the regulation is consisted with the statutory language. Section 29.3(e) is now entitled ''No Private Right of Action.''

Restrictions on Use of Protected CII in Civil Actions

The Department received three comments regarding the superfluous and potentially confusing use of the phrase ''for homeland security purposes'' in § 29.8(i). The Department agrees with these comments and has replaced that phrase with ''under the CII Act of 2002.''

FOIA Access and Mandatory Submission of Information

The Department received two comments pointing to ambiguities in § 29.3(a) and four comments supporting § 29.3(a). Comments sought to clarify through minor word changes that the provision was intended to prevent submitters from submitting material for protection under the CII Act of 2002 if the material already was required to be submitted to DHS under a Federal legal requirement. The Department agrees in significant part with the intent of the comments to distinguish between submissions of information to different agencies of the Federal government, consistent with the treatment of ''independently obtained information'' under section 214(c) of the statute, as is discussed in greater detail above. Therefore, § 29.3(a) has been modified accordingly.

Application of Various Laws and Executive Orders to This Interim Rulemaking

Good Cause for Immediate Effectiveness

DHS has determined that it is in the public interest to make this regulation effective upon publication in the **Federal Register**. DHS believes that information that would qualify as Protected CII and would assist DHS in implementing security measures is unlikely to be submitted to DHS before this regulation's effective date. After considering the likelihood that valuable information that likely is now being withheld because of fears that it might be handled without the protections that this regulation would prescribe, and the possibility that this information could be useful in deterring or responding to a security incident, DHS has concluded that the public interest is best served by making the regulation effective immediately.

Regulatory Evaluation

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601–612) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Office of Management and Budget directs agencies to assess the effect of regulatory changes on international trade. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State or local governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation.)

Executive Order 12866 Assessment

Executive Order 12866 (58 FR 51735, October 4, 1993), provides for making determinations whether a regulatory action is ''significant'' and therefore subject to Office of Management and Budget (OMB) review and to the requirements of the Executive Order.

DHS has determined that this action is a significant regulatory action within the meaning of Executive Order 12866 because there is significant public interest in security issues since the events of September 11, 2001.

DHS has performed an analysis of the expected costs of this interim rule. The interim rule affects entities in the private sector that have critical infrastructure information that they wish to share with DHS. The interim rule requires that, when DHS receives, validates, and shares CII, DHS and the receiving parties, whether they be other Federal agencies or State or local governments with whom DHS has signed agreements detailing the procedures on how Protected CII must be safeguarded, must take appropriate action to safeguard its contents and to destroy it when it is no longer needed. The interim rule does not require the use of safes or enhanced security equipment or the use of a crosscut shredder. Rather, the interim rule requires only that an affected entity or person restrict disclosure of, and access to, the protected information to those with a need to know, and destroy such information when it is no longer needed. Under the rule, a locked drawer or cabinet is an acceptable means of complying with the requirement to secure Protected CII, and a normal paper shredder or manual destruction are acceptable means of destroying Protected CII documents.

Costs

DHS believes that affected entities will incur minimal costs from complying with the interim rule because, in practice, affected entities already have systems in place for securing sensitive commercial, trade secret, or personnel information, which are appropriate for safeguarding Protected CII. For instance, a normal filing cabinet with a lock may be used to safeguard Protected CII, and a normal paper shredder or manual destruction may be used to destroy CII. Accordingly, the agency estimates that there will be minimal costs associated with safeguarding Protected CII.

The agency has estimated the following costs for placing the required protective marking and distribution

limitation statement on records containing Protected CII.

For an electronic document, a person can place the required markings on each page with a few keystrokes. The agency estimates that there will be no costs associated with this action.

For a document that is already printed, a person can use a rubber stamp for the required markings. Such stamps can be custom ordered and last several years. For the protective marking, the agency estimates that the cost of a rubber stamp is from $9.90 (for a stamp 4¼ inches wide by ¼ inch high) to $10.25 (for a stamp 5 inches wide by ¼ inch high). A typical ink pad costs approximately $15.60. A two-ounce bottle of ink for the ink pad costs about $3.75.

For other types of record, such as maps, photos, DVDs, CD–ROMs, and diskettes, a person can use a label for the required markings. Labels typically cost from $7.87 (for 840 multipurpose labels) to $22.65 (for 225 diskette inkjet labels) to $34.92 (for 30 DVC/CD–ROM labels). These labels can be pre-printed with the required markings, or the affected person can print the required markings on an as-needed basis.

The interim rule does not require a specific method for destroying Protected CII. Thus, a person may use any method of destruction, so long as it precludes recognition or reconstruction of the Protected CII. DHS believes that most affected entities already have the capability to destroy CII in accordance with the requirements in this interim final rule. Thus, the agency estimates that there will be no costs associated with these destruction requirements.

Accordingly, DHS believes that the costs associated with this interim rule are minimal; however, the Department will accept comments addressing the estimated costs associated with the implementation of this rule.

Benefits

The primary benefit of the interim rule will be DHS's ability to receive information from those with direct knowledge on the security of the United States' critical infrastructure, in order to reduce its vulnerability to acts of terrorism by ensuring that information pertaining to the security of critical infrastructure is properly safeguarded and protected from public disclosure. In addition, based on information shared, DHS will provide threat information, security directives, and information circulars throughout the Federal, State, and local governments, to law enforcement officials, to the private sector, and other persons that have a need to know, and to act upon, information about security concerns related to the nation's critical infrastructure.

Prior to providing Protected CII to entities, and to ensure that any information these entities produce that would be treated as Protected CII is safeguarded, DHS must ensure that those entities are under a legal obligation to protect Protected CII from disclosure.

DHS notes that the unauthorized disclosure of Protected CII can have a detrimental effect not only on the ability to thwart terrorist and other criminal activities in the transportation sector, but also on the willingness of the private sector to share that information with DHS if that information might be publicly disclosed.

The effectiveness of providing Protected CII to persons involved with the protection of this country's critical infrastructures, and of security measures developed by those persons, depends on strictly limiting access to the information to those persons who have a need to know. Given the minimal cost associated with this interim rule and the potential benefits of preventing, or mitigating the effects of, terrorist attacks on the United States' critical infrastructures, DHS believes that this interim final will be cost-beneficial; however, the Department will accept comments addressing the anticipated benefits associated with the implementation of this rule.

Initial Regulatory Flexibility Determination

The Regulatory Flexibility Act of 1980, as amended (RFA), was enacted to ensure that small entities are not unnecessarily or disproportionately burdened by Federal regulations. The RFA requires agencies to review rules to determine if they have a ''significant impact on a substantial number of small entities.'' DHS has reviewed this rule and has determined that it will not have a significant economic impact on a substantial number of small entities for the following reasons:

(1) In practice, affected entities already have systems in place for securing sensitive commercial, trade secret, or personnel information, which are appropriate for safeguarding Protected CII. For instance, a normal filing cabinet with a lock may be used to safeguard Protected CII, and a normal paper shredder or manual destruction may be used to destroy CII. Accordingly, the agency estimates that there will be minimal costs associated with safeguarding Protected CII.

(2) The agency has estimated the following costs for placing the required protective marking and distribution limitation statement on records containing Protected CII.

(a) For an electronic document, a person can place the required markings on each page with a few keystrokes. The agency estimates that there will be no costs associated with this action.

(b) For a document that is already printed, a person can use a rubber stamp for the required markings. Such stamps can be custom ordered and last several years. For the protective marking, the agency estimates that the cost of a rubber stamp is from $9.90 (for a stamp 4¼ inches wide by ¼ inch high) to $10.25 (for a stamp 5 inches wide by ¼ inch high). A typical ink pad costs approximately $15.60. A two-ounce bottle of ink for the ink pad costs about $3.75.

(c) For other types of record, such as maps, photos, DVDs, CD–ROMs, and diskettes, a person can use a label for the required markings. Labels typically cost from $7.87 (for 840 multipurpose labels) to $22.65 (for 225 diskette inkjet labels) to $34.92 (for 30 DVC/CD–ROM labels). These labels can be pre-printed with the required markings, or the affected person can print the required markings on an as-needed basis.

(3) The interim rule does not require a specific method for destroying Protected CII. Thus, a person may use any method of destruction, so long as it precludes recognition or reconstruction of the Protected CII. DHS believes that most affected entities already have the capability to destroy CII in accordance with the requirements in this interim rule. Thus, the agency estimates that there will be no costs associated with these destruction requirements; however, the Department will accept comments addressing the impact on small entities associated with the implementation of this rule.

Unfunded Mandates Reform Act of 1995

This interim rule will not result in the expenditure by State and local governments, in the aggregate, or by the private sector, of $100 million or more in any one year, and it will not significantly or uniquely affect small governments.

Executive Order 13132—Federalism

The Department of Homeland Security does not believe this interim rule will have substantial direct effects on the States, on the relationship between the national government and the States, or on distribution of power and responsibilities among the various levels of government. States will benefit, however, from this interim rule to the extent that Protected CII is shared with

them. The Department requests comment on the federalism impact of this interim rule.

Paperwork Reduction Act of 1995

Under the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501–3520), a Federal agency must obtain approval from the Office of Management and Budget (OMB) for each collection of information it conducts, sponsors, or requires through regulations. This rule does not contain provisions for collection of information, does not meet the definition of ''information collection'' as defined under 5 CFR part 1320, and is therefore exempt from the requirements of the PRA. Accordingly, there is no requirement to obtain OMB approval for information collection.

Environmental Analysis

DHS has analyzed this regulation for purposes of the National Environmental Policy Act and has concluded that this rule will not have any significant impact on the quality of the human environment.

List of Subjects in 6 CFR Part 29

Confidential business information, Reporting and recordkeeping requirements.

Authority and Issuance

■ For the reasons discussed in the preamble, 6 CFR chapter I is amended by adding part 29 to read as follows:

PART 29—PROTECTED CRITICAL INFRASTRUCTURE INFORMATION

Sec.

Authority: Pub. L. 107–296, 116 Stat. 2135 (6 U.S.C. 1 *et seq.*); 5 U.S.C. 301.

§ 29.1 Purpose and scope.

(a) *Purpose of the rule.* This part implements section 214 of Title II, Subtitle B, of the Homeland Security Act of 2002 through the establishment of uniform procedures for the receipt, care, and storage of Critical Infrastructure Information (CII) voluntarily submitted to the Federal government through the Department of Homeland Security. Title II, Subtitle B, of the Homeland Security Act is referred to herein as the Critical Infrastructure Information Act of 2002 (CII Act of 2002). Consistent with the statutory mission of the Department of Homeland Security (DHS) to prevent terrorist attacks within the United States and reduce the vulnerability of the United States to terrorism, it is the policy of DHS to encourage the voluntary submission of CII by safeguarding and protecting that information from unauthorized disclosure and by ensuring that such information is expeditiously and securely shared with appropriate authorities including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, and disrupting terrorist threats to our homeland. As required by the CII Act of 2002, the procedures established herein include mechanisms regarding:

(1) The acknowledgement of receipt by DHS of voluntarily submitted CII;

(2) The maintenance of the identification of CII voluntarily submitted to DHS for purposes of, and subject to the provisions of the CII Act of 2002;

(3) The receipt, handling, storage, and proper marking of information as Protected CII;

(4) The safeguarding and maintenance of the confidentiality of such information that permits the sharing of such information within the Federal government and with foreign, State, and local governments and government authorities, and the private sector or the general public, in the form of advisories or warnings; and

(5) The issuance of notices and warnings related to the protection of critical infrastructure and protected systems in such a manner as to protect from unauthorized disclosure the identity of the submitting person or entity as well as information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily available in the public domain.

(b) *Scope.* These procedures apply to all Federal agencies that handle, use, or store Protected CII pursuant to the CII Act of 2002. In addition, these procedures apply to United States Government contractors, to foreign, State, and local governments, and to government authorities, pursuant to any necessary express written agreements, treaties, bilateral agreements, or other statutory authority.

§ 29.2 Definitions.

For purposes of this part:

Critical Infrastructure has the definition referenced in section 2 of the Homeland Security Act of 2002 and 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.

Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems. CII consists of records and information concerning:

(1) Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms the interstate commerce of the United States, or threatens public health or safety;

(2) The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk-management planning, or risk audit; or

(3) Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Critical Infrastructure Information Program, or CII Program means the maintenance, management, and review of these procedures and of the information provided to DHS in furtherance of the protections provided by the CII Act of 2002.

Information Sharing and Analysis Organization, or ISAO means any formal or informal entity or collaboration created or employed by public or private sector organizations for purposes of:

(1) Gathering and analyzing CII in order to better understand security problems and interdependencies related to critical infrastructure and protected systems in order to ensure the

availability, integrity, and reliability thereof;

(2) Communicating or sharing CII to help prevent, detect, mitigate, or recover from the effects of an interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and

(3) Voluntarily disseminating CII to its members, Federal, State, and local governments, or to any other entities that may be of assistance in carrying out the purposes specified in this section.

Local Government has the same meaning as is established in section 2 of the Homeland Security Act of 2002 and means:

(1) A county, municipality, city, town, township, local public authority, school district, special district, intrastate district, council of governments (regardless of whether the council of governments is incorporated as a nonprofit corporation under State law), regional or interstate government entity, or agency or instrumentality of a local government;

(2) An Indian tribe or authorized tribal organization, or in Alaska a Native village or Alaska Regional Native Corporation; and

(3) A rural community, unincorporated town or village, or other public entity.

Protected Critical Infrastructure Information, or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in § 29.5. This information maintains its protected status unless DHS's Protected CII Program Manager or the Protected CII Program Manager's designees render a final decision that the information is not Protected CII.

Protected System 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 includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component 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.

Purpose of CII has the meaning set forth in section 214(a)(1) of the CII Act of 2002 and includes the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose.

Submission to DHS as referenced in these procedures means any transmittal of CII to the DHS Protected CII Program Manager or the Protected CII Program Manager's designees, as set forth in § 29.5.

Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information; such submission may be accomplished by (*i.e.*, come from) a single entity or by an ISAO acting on behalf of its members. In the case of any action brought under the securities laws—as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—the term ''voluntary'' does not include information or statements contained in any documents or materials filed, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(i)), with the Securities and Exchange Commission or with Federal banking regulators; and with respect to the submission of CII, it does not include any disclosure or writing that when made accompanies the solicitation of an offer or a sale of securities. The term also explicitly excludes information or statements submitted during a regulatory proceeding or relied upon as a basis for making licensing or permitting determinations.

§ 29.3 Effect of provisions.

(a) *Mandatory submissions of information.* The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to DHS pursuant to a Federal legal requirement, nor do they pertain to any obligation of any Federal agency to disclose mandatorily submitted information (even where it is identical to information voluntarily submitted to DHS pursuant to the CII Act of 2002). The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information to a Federal agency under any other provision of law. Information submitted to any other Federal agency pursuant to a Federal legal requirement is not to be marked as submitted or protected under the CII Act of 2002 or otherwise afforded the protection of the CII Act of 2002, provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002.

(b) *Freedom of Information Act disclosure exemptions.* Information that is separately exempt from disclosure under the Freedom of Information Act or applicable State or local law does not lose its separate exemption protection due to the applicability of these procedures or any failure to follow them.

(c) *Restriction on use of Protected CII by regulatory and other Federal agencies.* No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of that same information. Federal agencies shall not utilize Protected CII for regulatory purposes without the written consent of the submitter or another party on the submitter's behalf.

(d) *Independently obtained information.* These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local government entity, agency, or authority, or any third party, under applicable law, to otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

(e) *No private right of action.* Nothing contained in these procedures is intended to confer any substantive or procedural right or privilege on any person or entity. Nothing in these procedures shall be construed to create a private right of action for enforcement of any provision of these procedures or a defense to noncompliance with any independently applicable legal obligation.

§ 29.4 Protected Critical Infrastructure Information Program administration.

(a) *IAIP Directorate Program Management.* The Secretary of the Department of Homeland Security hereby designates the Under Secretary of the Information Analysis and Infrastructure Protection (IAIP)

Directorate as the senior DHS official responsible for the direction and administration of the Protected CII Program.

(b) *Appointment of a Protected CII Program Manager.* The Under Secretary for IAIP shall:

(1) Appoint a Protected CII Program Manager within the IAIP Directorate who is responsible to the Under Secretary for the administration of the Protected CII Program;

(2) Commit resources necessary to the effective implementation of the Protected CII Program;

(3) Ensure that sufficient personnel, including such detailees or assignees from other Federal national security, homeland security, or law enforcement entities as the Under Secretary deems appropriate, are assigned to the Protected CII Program to facilitate the expeditious and secure sharing with appropriate authorities, including Federal national security, homeland security, and law enforcement entities and, consistent with the CII Act of 2002, with State and local officials, where doing so may reasonably be expected to assist in preventing, preempting, or disrupting terrorist threats to our homeland; and

(4) Promulgate implementing directives and prepare training materials as appropriate for the proper treatment of Protected CII.

(c) *Appointment of Protected CII Officers.* The Protected CII Program Manager shall establish procedures to ensure that any DHS component or other Federal, State, or local entity that works with Protected CII appoints one or more employees to serve as a Protected CII Officer for the activity in order to carry out the responsibilities stated in paragraph (d) of this section. Persons appointed to these positions shall be fully familiar with these procedures.

(d) *Responsibilities of Protected CII Officers.* Protected CII Officers shall:

(1) Oversee the handling, use, and storage of Protected CII;

(2) Ensure the expeditious and secure sharing of Protected CII with appropriate authorities, as set forth in § 29.1(a) and paragraph (b)(3) of this section;

(3) Establish and maintain an ongoing self-inspection program, to include periodic review and assessment of the entity's handling, use, and storage of Protected CII;

(4) Establish additional procedures as necessary to prevent unauthorized access to Protected CII; and

(5) Ensure prompt and appropriate coordination with the Protected CII Program Manager regarding any request, challenge, or complaint arising out of the implementation of these procedures.

(e) *Protected Critical Infrastructure Information Management System (PCIIMS).* The Protected CII Program Manager or the Protected CII Program Manager's designees shall develop and use an electronic database, to be known as the ''Protected Critical Infrastructure Information Management System'' (PCIIMS), to record the receipt, acknowledgement, validation, storage, dissemination, and destruction of Protected CII. This compilation of Protected CII shall be safeguarded and protected in accordance with the provisions of the CII Act of 2002.

§ 29.5 Requirements for protection.

(a) CII shall receive the protections of section 214 of the CII Act of 2002 only when:

(1) Such information is voluntarily submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees;

(2) The information is submitted for use by DHS for the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purposes including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland, as evidenced below;

(3) The information is accompanied by an express statement as follows:

(i) In the case of written information or records, through a written marking on the information or records substantially similar to the following: ''This information is voluntarily submitted to the Federal government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002''; or

(ii) In the case of oral information, within fifteen calendar days of the oral submission, through a written statement comparable to the one specified above, and a certification as specified below, accompanied by a written or otherwise tangible version of the oral information initially provided; and

(4) The submitted information additionally is accompanied by a statement, signed by the submitting entity, certifying essentially to the following on behalf of the named entity:

(i) The submitter is voluntarily providing the information for the purposes of the CII Act of 2002;

(ii) The information being submitted is not being submitted in lieu of independent compliance with a Federal legal requirement;

(iii) The information is or is not required to be submitted to a Federal agency. If the information is required to be submitted to a Federal agency, the submitter shall identify the Federal agency requiring submission and the legal authority that mandates the submission; and

(iv) The information is of a type not customarily in the public domain.

(b) Information that is not submitted to the Protected CII Program Manager or the Protected CII Program Manager's designees will not qualify for protection under the CII Act of 2002. Any DHS component other than the IAIP Directorate that receives information with a request for protection under the CII Act of 2002, shall immediately forward the information to the Protected CII Program Manager. Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt and validate Protected CII pursuant to § 29.6(a).

(c) Federal agencies and DHS components other than the IAIP Directorate shall maintain information as protected by the provisions of the CII Act of 2002 when that information is provided to the agency or component by the Protected CII Program Manager or the Protected CII Program Manager's designees and is marked as required in § 29.6(c).

(d) All submissions seeking Protected CII status shall be regarded as submitted with the presumption of good faith on the part of the submitter.

(e) Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

§ 29.6 Acknowledgment of receipt, validation, and marking.

(a) *Authorized officials.* Only the Protected CII Program Manager or the Protected CII Program Manager's designees are authorized to acknowledge receipt of and validate information as Protected CII.

(b) *Presumption of protection.* All information submitted in accordance with the procedures set forth herein will be presumed to be and will be treated as Protected CII from the time the information is received by DHS, either through the DHS component or the Protected CII Program Manager or the Protected CII Program Manager's designees. The information shall remain protected unless and until the Protected CII Program Manager or the Protected CII Program Manager's designees render

a final decision that the information is not Protected CII.

(c) *Marking of information.* In addition to markings made pursuant to § 29.5(a) by submitters of CII requesting review, all Protected CII shall be clearly identified through markings made by the Protected CII Program Manager or the Protected CII Program Manager's designees. The Protected CII Program Manager or the Protected CII Program Manager's designees shall mark Protected CII materials as follows: ''This document contains Protected CII. In accordance with the provisions of 6 CFR part 29, it is exempt from release under the Freedom of Information Act (5 U.S.C. 552(b)(3)). Unauthorized release may result in civil penalty or other action. It is to be safeguarded and disseminated in accordance with Protected CII Program requirements.''

(d) *Acknowledgement of receipt of information.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall acknowledge receipt of information submitted as CII and accompanied by an express statement and certification, and in so doing shall:

(1) Contact the submitter, within thirty calendar days of receipt, by the means of delivery prescribed in procedures developed by the Protected CII Program Manager or the Protected CII Program Manager. In the case of oral submissions, receipt will be acknowledged in writing within thirty calendar days after receipt by the Protected CII Program Manager or the Protected CII Program Manager's designees of a written statement, certification, and documentation of the oral submission, as referenced in § 29.5(a)(3)(ii);

(2) Maintain a database including date of receipt, name of submitter, description of information, manner of acknowledgment, tracking number, and validation status; and

(3) Provide the submitter with a unique tracking number that will accompany the information from the time it is received by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(e) *Validation of information.*

(1) The Protected CII Program Manager or the Protected CII Program Manager's designees shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Protected CII Program Manager or the Protected CII Program Manager's designee shall review the submitted information as soon as practicable. If a determination is made that the submitted information meets the requirements for protection, the Protected CII Program Manager or the Protected CII Program Manager's designee shall mark the information as required in paragraph (c) of this section, and disclose it only pursuant to § 29.8.

(2) If the Protected CII Program Manager or the Protected CII Program Manager's designees make an initial determination that the information submitted does not meet the requirements for protection under the CII Act of 2002, the Protected CII Program Manager or the Protected CII Program Manager's designees shall:

(i) Notify the submitter of the initial determination that the information is not considered to be Protected CII. This notification also shall:

(A) Request that the submitter further explain the nature of the information and the submitter's basis for believing the information qualifies for protection under the CII Act of 2002;

(B) Advise the submitter that the Protected CII Program Manager or the Protected CII Program Manager's designees will review any further information provided before rendering a final determination;

(C) Provide the submitter with an opportunity to withdraw the submission;

(D) Notify the submitter that any response to the notification must be received by the Protected CII Program Manager or the Protected CII Program Manager's designees no later than thirty calendar days after the date of the notification; and

(E) Request the submitter to state whether, in the event the Protected CII Program Manager or the Protected CII Program Manager's designees make a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

(ii) If the Protected CII Program Manager or the Protected CII Program Manager's designees, after following the procedures set forth in paragraph (e)(2)(i) of this section, make a final determination that the information is not Protected CII, the Protected CII Program Manager or the Protected CII Program Manager's designees, in accordance with the submitter's written preference, shall maintain the information without protection or following coordination, as appropriate, with other Federal national security, homeland security, or law enforcement authorities, destroy it in accordance with the Federal Records Act unless the Protected CII Program Manager or the Protected CII Program Manager's designees, consistent with the coordination required in this subpart, determine there is a need to retain it for law enforcement and/or national security reasons. The Protected CII Program Manager or the Protected CII Program Manager's designees shall destroy the information within thirty calendar days of making a final determination. If the submitter, however, cannot be notified or the submitter's response is not received within thirty calendar days after the submitter received the notification, as provided in paragraph (e)(2)(i) of this section, the Protected CII Program Manager or the Protected CII Program Manager's designee will destroy the information in accordance with the Federal Records Act, unless the Protected CII Program Manager or the Protected CII Program Manager's designee, after coordination with other Federal national security, homeland security, or law enforcement authorities, as appropriate, determines that there is a need to retain it for law enforcement and/or national security reasons.

(f) *Changing the status of Protected CII to non-Protected CII.* Once information is validated, only the Protected CII Program Manager or the Protected CII Program Manager's designees may change the status of Protected CII to that of non-Protected CII and remove its Protected CII markings. Status changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation. The Protected CII Program Manager or the Protected CII Program Manager's designees shall inform the submitter when a change in status is made. Notice of the change in status of Protected CII shall be provided to all recipients of that Protected CII under § 29.8.

§ 29.7 Safeguarding of Protected Critical Infrastructure Information.

(a) *Safeguarding.* All persons granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Protected CII shall be protected at all times by appropriate storage and handling. Each person who works with Protected CII is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

(b) *Use and storage.* When Protected CII is in the physical possession of a person, reasonable steps shall be taken to minimize the risk of access to Protected CII by unauthorized persons. When Protected CII is not in the physical possession of a person, it shall be stored in a secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity.

(c) *Reproduction.* Pursuant to procedures prescribed by the Protected CII Program Manager, a document or other material containing PCII may be reproduced to the extent necessary consistent with the need to carry out official duties, provided that the reproduced documents or material are marked and protected in the same manner as the original documents or material.

(d) *Disposal of information.* Documents and material containing Protected CII may be disposed of by any method that prevents unauthorized retrieval.

(e) *Transmission of information.* Protected CII shall be transmitted only by secure means of delivery as determined by the Protected CII Program Manager or the Protected CII Program Manager's designees.

(f) *Automated Information Systems.* The Protected CII Program Manager or the Protected CII Program Manager's designees shall establish security requirements for Automated Information Systems that contain Protected CII.

§ 29.8 Disclosure of Protected Critical Infrastructure Information.

(a) *Authorization of access.* The Under Secretary for IAIP, or the Under Secretary's designee, may choose to provide or authorize access to Protected CII when it is determined that this access supports a lawful and authorized Government purpose as enumerated in the CII Act of 2002, other law, regulation, or legal authority. Any disclosure or use of Protected CII within the Federal government is limited by the terms of the CII Act of 2002. Accordingly, any advisories, alerts, or warnings issued to the public pursuant to paragraph (e) of this section shall protect from disclosure:

(1) The source of any voluntarily submitted CII that forms the basis for the warning, and

(2) Any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(b) *Federal, State, and local government sharing.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to an employee of the Federal government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose including, without limitation, the identification, analysis, prevention, preemption, and/or disruption of terrorist threats to our homeland. Protected CII may be provided to a State or local government entity only pursuant to its express written agreement with the Protected CII Program Manager to comply with the requirements of paragraph (d) of this section and that acknowledges the understanding and responsibilities of the recipient.

(c) *Disclosure of information to Federal contractors.* Disclosure of Protected CII to Federal contractors may be made only after the Protected CII Program Manager or a Protected CII Officer certifies that the contractor is performing services in support of the purposes of DHS, the contractor has signed corporate or individual confidentiality agreements as appropriate, covering an identified category of contractor employees where appropriate, and has agreed by contract to comply with all the requirements of the Protected CII Program. The contractor shall safeguard Protected CII in accordance with these procedures and shall not remove any ''Protected CII'' markings. Contractors shall not further disclose Protected CII to any of their components, additional employees, or other contractors (including subcontractors) without the prior written approval of the Protected CII Program Manager or the Protected CII Program Manager's designees, unless such disclosure is expressly authorized in writing by the submitter and is the subject of timely notification to the Protected CII Program Manager.

(d) *Further use or disclosure of information by State and local governments.*

(1) State and local governments receiving information marked ''Protected Critical Infrastructure Information'' shall not share that information with any other party, or remove any Protected CII markings, without first obtaining authorization from the Protected CII Program Manager or the Protected CII Program Manager's designees who shall be responsible for requesting and obtaining written consent for any such State or local government disclosure from the person or entity that submitted the information or on whose behalf the information was submitted.

(2) The Protected CII Program Manager or a Protected CII Program Manager's designee may not authorize State and local governments to further disclose the information to another party unless the Protected CII Program Manager or a Protected CII Program Manager's designee first obtains the written consent of the person or entity submitting the information.

(3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

(e) *Disclosure of information to appropriate entities or to the general public.* The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any Protected CII that forms the basis for the warning as well as any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain.

(f) *Access by Congress and whistleblower protection.*

(1) Exceptions for disclosure.

(i) Pursuant to section 214(a)(1)(D) of the CII Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except—

(A) In furtherance of an investigation or the prosecution of a criminal act; or

(B) When disclosure of the information is made—

(*1*) To either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(*2*) To the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(ii) If any officer or employee of the United States makes any disclosure pursuant to these exceptions, contemporaneous written notification must be provided to the Department through the Protected CII Program Manager.

(2) Consistent with the authority to disclose information for any purpose described in § 29.2, disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security.

(3) Subject to the limitations of title 5 U.S.C., section 1213 (the ''Whistleblower Protection Act''), disclosure of Protected CII may be made by any officer or employee of the United States who reasonably believes that such information:

(i) Evidences an employee's or agency's conduct in violation of criminal law, or any other law, rule, or regulation, affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution or

(ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution.

(4) Disclosures of all of the information cited in paragraphs (f)(1) through (3) of this section, including under paragraph (f)(1)(i)(A), are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

(g) *Responding to requests made under the Freedom of Information Act or State/local information access laws.*

(1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the Protected CII Program Manager or the Protected CII Program Manager's designees to a State or local government agency, entity, or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the Protected CII Program Manager, who shall in turn consult with the DHS Office of the General Counsel.

(2) These procedures do not limit or otherwise affect the ability of a State or local government entity, agency, or authority to obtain under applicable State or local law information directly from the same person or entity voluntarily submitting information to DHS. Information independently obtained by a State or local government entity, agency, or authority is not subject to the CII Act of 2002's prohibition on making such information available pursuant to any State or local law requiring disclosure of records or information.

(h) *Ex parte communications with decisionmaking officials.* Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official.

(i) *Restriction on use of Protected CII in civil actions.* Pursuant to section 214(a)(1)(C) of the Homeland Security Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used directly by any Federal, State, or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith under the CII Act of 2002.

(j) *Disclosure to foreign governments.* The Protected CII Program Manager or the Protected CII Program Manager's designees may provide Protected CII to a foreign Government without the written consent of the person or entity submitting such information to the same extent, and under the same conditions, it may provide advisories, alerts, and warnings to other governmental entities as described in paragraph (e) of this section, or in furtherance of an investigation or the prosecution of a criminal act. Before disclosing Protected CII to a foreign government, the Protected CII Program Manager or the Protected CII Program Manager's designees shall protect from disclosure the source of the Protected CII, any information that is proprietary or business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriate for such disclosure.

(k) *Obtaining written consent for further disclosure from the person or entity submitting information.*

(1) Authority to Seek and Obtain Submitter's Consent to Disclosure. The Protected CII Program Manager or any Protected CII Program Manager's designee may seek and obtain written consent from persons or entities submitting information when such consent is required under the CII Act of 2002 to permit disclosure. In exigent circumstances, and so long as contemporaneous notice is provided to the Protected CII Program Manager or the Protected CII Program Manager's designees, any Federal government employee may seek the consent of the submitting party to the disclosure of Protected CII where such consent is required under the CII Act of 2002.

(2) Consequence of Consent. Whether given in response to a request from the Protected CII Program Manager, the Protected CII Program Manager's designees, or another Federal government employee pursuant to paragraph (k)(1) of this section, a person's or entity's consent to additional disclosure, if conditioned on a limited release of Protected CII that is made for DHS's purposes and in a manner that offers reasonable protection against disclosure to the general public, shall not result in the information's loss of treatment as Protected CII.

§ 29.9 Investigation and reporting of violation of protected CII procedures.

(a) *Reporting of possible violations.* Persons authorized to have access to Protected CII shall report any possible violation of security procedures, the loss or misplacement of Protected CII, and any unauthorized disclosure of Protected CII immediately to the Protected CII Program Manager or the Protected CII Program Manager's designees who shall in turn report the incident to the IAIP Directorate Security Officer and to the DHS Inspector General.

(b) *Review and investigation of written report.* The Inspector General, Protected CII Program Manager, or IAIP Security Officer shall investigate the incident and, in consultation with the DHS Office of the General Counsel, determine whether a violation of procedures, loss of information, and/or unauthorized disclosure has occurred. If the investigation reveals any evidence of wrongdoing, DHS, through its Office of the General Counsel, shall immediately contact the Department of Justice's Criminal Division for consideration of prosecution under the criminal penalty provisions of section 214(f) of the CII Act of 2002.

(c) *Notification to originator of Protected CII.* If the Protected CII Program Manager or the IAIP Security Officer determines that a loss of information or an unauthorized disclosure has occurred, the Protected CII Program Manager or the Protected CII Program Manager's designees shall notify the submitter of the information in writing, unless providing such notification could reasonably be expected to harm the investigation of that loss or any other law enforcement, national security, or homeland security interest. The written notice shall contain a description of the incident and the date of disclosure, if known.

(d) *Criminal and administrative penalties.* As established in section 214(f) of the CII Act, whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information protected from disclosure by the CII Act of 2002 and coming to the officer or employee in the course of his or her employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than one year, or both, and shall be removed from office or employment.

Dated: February 12, 2004.

Tom Ridge,

Secretary of Homeland Security.

[FR Doc. 04–3641 Filed 2–19–04; 8:45 am]

BILLING CODE 4410–10–P