

# THE FINANCIAL SERVICES ROUNDTABLE



**BITS**  
FINANCIAL SERVICES  
R O U N D T A B L E

May 20, 2004

Janice Pesyna  
Office of the General Counsel  
Department of Homeland Security  
Washington, D.C. 20528

Re: Procedures for Handling Critical Infrastructure Information: Interim Rule,  
RIN 1601-AA14

Dear Ms. Pesyna:

The Financial Services Roundtable (the “Roundtable”) and BITS appreciate the opportunity to comment to the Department of Homeland Security (“DHS”) on the Procedures for Handling Critical Infrastructure Information: Interim Rule.

BITS and the Roundtable share membership; their members are 100 of the largest integrated financial services institutions providing banking, insurance and investment products and services to American consumers and corporate customers. BITS serves as the strategic brain trust for the financial services industry where commerce, financial services and technology intersect. The Roundtable is an advocacy and lobbying organization, using grassroots power, knowledge and experience to help shape public policy.

BITS and Roundtable members continue to work proactively on industry-wide and inter-sector efforts to strengthen our preparedness for—and our ability to react to and recover from—future terrorist or other attacks. A fundamental part of this process involves communication with regulatory agencies and other relevant federal, state and local agencies to ensure a cooperative and coordinated response to any future events. We support the mission of both the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (the “FSSCC”) and the Financial and Banking Information Infrastructure Committee (“FBIIC”), which provide leadership to our sector. We also work closely with the Financial Services Information Sharing and Analysis Center (“FS/ISAC”).

## **General Comments**

The purpose of the rule is to establish “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.” This comment letter summarizes key concerns about the interim rule and related issues that BITS and the Roundtable would like DHS to consider. Individual members of BITS and the Roundtable may also respond with separate comment letters.

BITS and the Roundtable commend DHS for taking a leadership role to establish a mechanism for the private sector to share proprietary and confidential information with the U.S. government in order to gain a better understanding of threats to, attacks upon, and vulnerabilities within the nation’s critical infrastructure. BITS and the Roundtable strongly support an exemption from the Freedom of Information Act (“FOIA”) as a necessary step for the private sector to submit sensitive or confidential information to DHS in the interest of protecting the nation’s citizens and critical infrastructure.

On February 27, 2004, Fred Herr, Program Manager at the DHS Protected Critical Infrastructure Information Program Office, provided an overview of the interim rule to the BITS Crisis Management Coordination Working Group. BITS appreciates Mr. Herr’s participation in that conference call and his willingness to respond to members’ questions.

BITS and Roundtable members support the central purpose of the interim rule but have some concerns with the scope and implementation of the rule. As a general matter, BITS and Roundtable members are very concerned about the controls that DHS and others, such as contractors, will have in place to protect critical infrastructure entities including employees and customers of financial institutions. Individuals entrusted to implement this program must be mindful of the potential impact that an intentional or accidental release of critical infrastructure information might have on individuals, companies and the government. Unlawful disclosure of sensitive information may result in irreparable harm to individuals, organizations and the critical infrastructure. Disclosures also could undermine the entire CII program if DHS fails to establish and maintain a trusted environment.

The rule indicates that subsequent phases will expand the points of entry for information within DHS. Eventually, agreements with additional entities will be reached and the disclosure of information will expand to other federal, state, and local government entities, and eventually to foreign governments. Without adequate protection, the value of this rule will be sharply limited. As the adage goes, “all disasters are local.” Protection of individual components of critical infrastructure sectors and response to the majority of crises will take place at the

state and local level. BITS and Roundtable members strongly urge DHS to undertake a strategy that extends the protection of this rule to the state and local levels as soon as possible. The model of protection at these levels should include not only information shared with DHS, but also information initially provided at the local or state level.

### **Definitions (Section 29.2)**

BITS and Roundtable members request that the definition of “critical infrastructure information” be modified. The current definition focuses heavily on information concerning the security of the critical infrastructure, including threats, incidents, vulnerabilities, assessments, and mitigation plans and efforts. The current definition does not make explicit reference to information provided concerning the critical infrastructure component, such as the asset or system that is the object of the security measures or concerns, which may include component designs, architecture, business plans, external interfaces, communications facilities, etc. The category of information that describes the infrastructure component also needs to be addressed explicitly in the procedures. In addition, we recommend that the first sentence of the definition be changed to read as follows: “ ‘Critical Infrastructure Information’ or ‘CII’ connotes sensitive information that should not be available in the public domain as it is related to the security of critical infrastructure or protected systems.”

To meet the definition of CII, information must relate to critical infrastructure protection or protected systems and fall under the categories of threats, vulnerabilities, and/or the security state of networks. BITS and Roundtable members are concerned that the rule does not contain enough guidance as to what constitutes a reportable event or situation and the specific format of the submission, including what items should be incorporated, and what level of detail is required. The definition states “networks” but makes no mention of their connected subsystems and business applications.

### **Requirements for Protection (Sec 29.5)**

The interim rule in section 29.5(d)(2) states: “The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information.” In 29.6(e)(1)(ii) the rule notes that, if the CII Program Manager determines the information does not meet requirements under the provisions and is not Protected CII, the CII Program Manager can either maintain information without protections or can dispose of information in accordance with the Federal Records Act. BITS and Roundtable

members urge DHS to notify the submitter when information is deemed ineligible for protection and either destroy the information or seek the approval from the submitter to maintain the information without protections. This modification would help to provide assurance to the private sector that the information will be used only for the intended purpose.

### **Submission of Information**

The interim rule states that submissions must be submitted and signed by an individual of a submitting entity. However, there is no specific requirement in the interim rule that specifies who is considered an authorized individual of a submitting entity. BITS and Roundtable members are concerned that any individual within the financial services sector could submit information without appropriate authorization. DHS should establish parameters as to who is eligible to submit on behalf of an institution in order to protect the information and resulting harm to the institution. Moreover, BITS and the Roundtable urge DHS to conduct sufficient due diligence in validating the information up front and implementing strong security controls over logical and physical access to and storage of CII.

Based on Fred Herr's presentation, we understand that submissions can be made anonymously. Anonymous submissions pose significant challenges in validating information and limit the ability of DHS officials to seek clarification or to follow-up with submitters. While BITS and Roundtable members support provisions in the interim rule that permit ISACs to submit CII information to DHS, it is important for DHS to understand that efforts to undermine the anonymous features of the FS/ISAC would likely result in financial institutions from not submitting information to the FS/ISAC anonymously. The proposed rule does not specify if submissions can be made anonymously via Information Sharing and Analysis Centers (ISACs). While BITS and Roundtable members support the ability of ISACs to submit CII information to DHS on behalf of its members, we realize that validation and clarification of material submitted would be difficult if done so anonymously. However, it is critical that the anonymity provided by the FS/ISAC submission process be protected so as not to discourage sharing of information within the FS/ISAC community.

*Mandatory Submissions.* “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.” BITS and Roundtable members are concerned that mandatory submissions to regulatory agencies will be subject to FOIA. Involuntary information submitted should be granted the same level of anonymity as provided for voluntary submission through the FS/ISAC.

## **Sharing of Information Among Regulatory Agencies.**

The rule needs to further address how CII information will be shared among regulatory agencies and protected from disclosure. DHS needs to explain whether and how regulatory agencies could share highly confidential information with other federal agencies regardless of whether the information was or was not received in CII form. For example, DHS must detail how mandatory Suspicious Activity Reports (“SARs”) submitted to regulatory agencies and law enforcement agencies will be treated under the final rule. Additionally, results from regulatory audits and/or exams should not be disclosed.

## **Use of Submitted Information**

While the rule states that DHS will analyze the information provided by the private sector under the CII program, it does not provide detail on how this information will be analyzed or if the submitter would be apprised of how the information is being used. Additionally, the interim rule does not address the submitter’s (as a subject matter expert) or private-sector entities’ involvement in the analysis of the information provided. Misinterpreting information is a significant risk. For DHS or other government entities to understand the impact, it is imperative that subject matter experts be involved.

DHS should consider and explain how the private sector can be involved in the analysis process. For example, if a private-sector company official believes that the nation’s critical infrastructure is extremely vulnerable to an attack on a telecommunications facility because a potential single point of failure exists at the facility, what would DHS do with this information? Similarly, if DHS were informed that certain software vulnerabilities could be exploited to cripple the critical infrastructure, how would DHS respond?

BITS and Roundtable members believe that DHS should notify submitters of information when DHS determines that the information is not critical and either return the information or provide confirmation that the information has been destroyed when it no longer meets this definition. BITS and Roundtable members do not believe it is appropriate for DHS to hold non-critical information about the nation’s infrastructure for law enforcement or other purposes not directly related to the statute.

Misuse of information would undoubtedly lead to distrust of the program and undermine its effectiveness. To make this program a success, it is important that DHS focus on its core purpose of protecting the critical infrastructure and not act as a conduit for meeting other law-enforcement objectives.

## **Penalties for Misuse of Submitted Information**

The interim rule states that penalties for intentional misuse and/or mishandling of information by a federal employee can include fines and/or imprisonment for up to one year and loss of employment. BITS and Roundtable members recognize that the penalties are based on the statute. Nonetheless, BITS and Roundtable members urge DHS to apply the most stringent penalties for unauthorized disclosure. Since DHS has not established agreements with state, local, or foreign governments, BITS and Roundtable members are concerned about the efficacy of this provision of the program. Given the risks involved, it is imperative that anyone who receives and/or handles the information act responsibly in safeguarding its contents and adhering to the processes as stated by the rule. This includes government employees as well as contractors and others who might have access to the information.

*29.8(f) Access by Congress and whistleblower protection.* This section provides undesirable exceptions as to the disclosure restrictions; notably, if the information is pertinent to a criminal investigation or proceeding, for Congressional or Comptroller General disclosure, or when there is reason to believe there is criminal conduct, mismanagement, abuse of authority, etc. It is not clear in (f) if the written consent is required for the exception to occur or if the consent is needed to use the information for purposes other than those originally intended. However, it seems to state the Protected CII can be used for other purposes without consent for the cases noted in (f)(1) and (f)(2). BITS and Roundtable members believe the exceptions should be narrow.

*29.8(j) Disclosure to foreign governments.* Although the rule requires foreign governments to abide by the same restrictions, the information may be subject to disclosure in the foreign country if it is pertinent to a criminal investigation or the other country provides for other undesirable exceptions. This represents another circumstance in which CII might be disclosed to those for whom it is not intended.

## **Cost of Compliance**

BITS and Roundtable members believe that the interim rule underestimates the cost impact of complying with this rule, especially the cost of reviewing the rule and the decision-making process, since it will likely involve substantial review by legal counsel. The interim rule states that the cost of compliance for affected entities will be minimal: "... 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." DHS limits costs to use of locking filing cabinets, paper shredders (or other means to destroy proprietary and

confidential information), and costs for placing the required protective marking and distribution such as electronic marking, rubber stamps, and cost of transmission of information via standard mail, courier, etc. Costs enumerated are likely to be dwarfed by the cost of staff time required to respond, particularly if the submission has to be processed through the legal department. Moreover, the interim rule appears to ignore the costs for logical security protection (administration and storage). For most organizations, sensitive information will be stored and processed through information technology tools, not locked in a file cabinet. BITS and Roundtable members request that these additional costs be recognized in the final rule.

### **Related Concerns and Recommendations**

The CII final rule will be just one tool the government could use to identify threats, vulnerabilities and risks. BITS and Roundtable members want to remind DHS officials of other related issues that should be addressed to strengthen the resiliency of the nation's critical infrastructure.

*Address Critical Interdependencies.* BITS and Roundtable members urge DHS to focus on interdependencies among critical infrastructure providers. For example, a significant vulnerability that surfaced during 9/11 was the dependence on telecommunications providers. Recent government policies and actions have concluded that the telecommunications infrastructure underlying the critical financial services clearing, payment and settlement processes is a matter of national security. The financial services sector is dependent on resilient and robust telecommunications services. The financial services sector strongly emphasizes the need to maintain diversity as one of the components of resiliency. The primary challenges the financial services sector faces with respect to diversity are (a) failure of critical services due to the loss of diversity; (b) the ability to ensure that diversity is predictable and continually maintained; and (c) the potential for lack of clear understanding of terms and conditions in telecommunications contracts or tariffs (and the potential for resulting confusion when financial services institutions establish business continuity plans).

BITS has worked closely with its members, telecommunications companies, other sector associations, and representatives of federal agencies to outline the risks and mitigation strategies. These are complex problems that require close collaboration across critical infrastructure sectors and with federal, state and local governments. BITS and Roundtable members strongly encourage DHS to focus on identifying and mitigating risks due to interdependencies and to support public policy options that would invest in mitigating these risks. To this end, DHS should involve leaders from critical infrastructure sectors to examine infrastructure

vulnerabilities. DHS has an important role to play in supporting cross-sector collaboration. If structured properly (e.g., non-disclosure agreements, antitrust guidelines), private-sector firms can also play an important role in helping to identify and mitigate risks.

*Improve Information Sharing.* BITS and Roundtable members encourage the Administration to implement effective information exchanges between the government and the financial services sector. We do not want the CII program to be a “one-way street” in which the private sector provides information but rarely receives information that may be helpful in responding to risks. BITS and Roundtable members also support efforts to establish more robust information-sharing processes (such as those of the FS/ISAC) that quickly and securely provide information and analysis on cyber security vulnerabilities, risks, and risk-mitigation strategies to a larger universe of financial services organizations.

*Address Software Security Concerns.* BITS and Roundtable members encourage DHS to call on software vendors to be more accountable for the quality of their products. Software providers should accept responsibility for their role in supporting financial institutions and other critical infrastructure companies. To this end, BITS and the Roundtable want software and hardware vendors to: (1) provide a higher duty of care when selling to the financial industry and other critical infrastructure companies; (2) ensure products comply with security guidelines before releasing products; and (3) make the patch-management process more secure and efficient for organizations. These objectives are outlined in greater detail in the attached policy statement and “Business Requirements for Software Security and Patch Management.” BITS and the Roundtable support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software-development processes and sustain long-term R&D efforts to support stronger security in software products. BITS and Roundtable members also will seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for the software and hardware they purchase. Attached is the BITS and FSR policy statement on software security and business requirements for software security and patch management.

If you have any further questions or comments on this matter, please do not hesitate to contact us, John Beccia (FSR) or John Carlson (BITS) at (202) 289-4322.

Sincerely,

A handwritten signature in black ink that reads "Catherine A. Allen". The signature is written in a cursive style with a large initial 'C'.

Catherine A. Allen  
CEO, BITS

A handwritten signature in black ink that reads "Richard M. Whiting". The signature is written in a cursive style with a large initial 'R'.

Richard M. Whiting  
Executive Director and General Counsel  
The Financial Services Roundtable

Attachment

# BITS

FINANCIAL SERVICES  
R O U N D T A B L E

---

## SOFTWARE SECURITY

---

Security is a fundamental building block for all financial services. It is also a regulatory requirement. The financial services industry relies upon software to operate complex systems and provide services, as well as to protect customer information.

Financial services companies comply with a host of legal and regulatory requirements to ensure the privacy and security of customer information. Recently, the prevalence of security risks, threats and viruses, combined with a lack of accountability for software vulnerabilities, has saddled financial institutions with significant risks and skyrocketing costs.

In early 2004, BITS surveyed its members to estimate the costs to financial institutions of addressing software security and patch-management problems. Based on the survey, BITS and Financial Services Roundtable members pay an estimated \$400 million annually to deal with software security and patch management. Extrapolated to the entire financial services industry, these costs are approaching \$1 billion annually.

The members of BITS and The Financial Services Roundtable believe:

- Because the financial services industry plays a central role in the nation's critical infrastructure and is dependent on the products and services of software providers, such providers of mission critical software to the financial services industry need to accept responsibility for the role their products and services play in supporting the nation's critical infrastructure and should exhibit and be held to a "higher duty of care" to satisfy their own critical infrastructure responsibilities.
- Software vendors should ensure their products are designed to include security as part of the development process using security-trained and security-certified developers on product development and lifecycle teams.
- Software vendors should ensure through testing that their products meet quality standards and that financial services security requirements are met before products are sold.
- Software providers should develop patch-management processes that minimize costs, complexity, downtime, and risk to user organizations. Software vendors should identify vulnerabilities as soon as possible and ensure that the patch is thoroughly tested.
- Software vendors should continue patch support for older, but still viable, versions of software.

- Collaboration and coordination among other critical infrastructure sectors and government agencies are essential to mitigate software security risks.

The members of BITS and The Financial Services Roundtable:

- Support measures that make producers of software more accountable for the quality of their products.
- Support incentives (e.g., tax incentives, cyber-insurance, liability/safe harbor/tort reform, certification programs) and other measures that encourage implementation of more secure software development processes and sustain long-term R&D efforts to support stronger security in software products.
- Seek protection from U.S. antitrust laws for critical infrastructure industry groups that agree on baseline security specifications for software and hardware that they purchase.
- Encourage regulatory agencies to explore supervisory tools to ensure that critical third-party service providers and software vendors deliver safe and sound products to the financial services industry.
- Support and incorporate, where possible, the BITS Product Security Criteria into security policies, and encourage technology vendors to test products to meet these criteria.
- Apply a risk-management approach to software security by assessing risks and applying appropriate tools and best practices to ensure the most secure deployment and application of software possible across the entire enterprise.
- Participate in and support efforts to strengthen the Financial Services Information Sharing and Analysis Center (FS/ISAC) in order to share vulnerability information on the products deployed by financial institutions.
- Educate policy makers on the significance of the risks posed to the financial services sector and other critical infrastructure industries and the need to take action to mitigate these risks.

**BUSINESS REQUIREMENTS  
FOR  
SOFTWARE SECURITY AND PATCH MANAGEMENT**

Members of BITS and The Financial Services Roundtable believe software vendors should take responsibility for the quality of their products. Especially when selling products to companies that are within critical infrastructure industries, certain minimum requirements should be met. Following are recommended critical infrastructure sector Business Requirements.

**Provide a higher “duty of care” when selling to critical infrastructure industry companies.**

To meet this higher duty of care, vendors should:

- Make security a fundamental component of software design.
- Support older versions of software (e.g., NT), particularly if existing programs are functional and not past the end of their estimated life cycle.
- Make upgrading easier, less cumbersome and less costly, and offer more support.
  - Products should be less prone to failure and have an automated back-out feature.
  - Components (including embedded components used in other products) should be clearly defined in order for the customer to assess the cascading effect of the upgrade or installation.
- Publish metrics on security of new and existing products.
- Expand coordination and establish better communication with individual clients and industry groups.
  - Vendors should give customers an aggressive “patch playbook” which would provide clear guidance and explicit instructions for risk mitigation throughout the patch management process and especially in times of crisis.
  - Vendors should offer critical infrastructure customers access to one-on-one, private, early vulnerability notice prior to notifying the general public, possibly by establishing “preferred” customer levels. (Some vendors offer financial institutions advanced notification if they agree to serve as a “beta” site, however, this is not practical as an industry-wide solution.)
- Provide better security-trained and security-certified developers on product teams.
- Establish Regional Centers of Excellence to service major financial institutions in their area. Centers would keep IT profiles for each institution in order to:
  - Inform institutions of the likely effects of a new vulnerability on their specific IT environment.
  - Continually advise institutions on how to best apply patches.
  - Expedite patch installation by visiting the financial institution site.
  - Make on site or remote consultation available when patches affect other applications.

### **Comply with security requirements before releasing software products.**

Vendors should:

- Meet minimum security criteria, such as BITS software security criteria and/or the Common Criteria.
- Thoroughly test software products, taking into consideration that:
  - Testing needs to address both quality assurance as well as functionality against known and unknown threats.
- Conduct code reviews.
  - Whether conducted internally or outsourced, code reviews should involve tools or processes, such as code profilers and threat models, to ensure code integrity.

### **Improve the patch-management process to make it more secure and efficient and less costly to organizations.**

Vendors should:

- Issue patch alerts as early as possible.
- Continue patch support for older software.
  - Vendors should be clear about the level of support provided for each software version.
  - Vendors are strongly encouraged to provide support for up to two versions of older software, i.e., the N-2 level.
- Provide automatic, user-controlled patch-management systems, such as uniform, reliable, and, possibly, industry-standard installers.
- Ensure all patches come with an automated back-out function and do not require reboots.
- Support clients who purchase third-party installer tools (until a standard is established).
- Thoroughly test patches before release.
  - Testing should include patch-to-patch testing to identify any cascade effects and in-depth compatibility testing for effects on networks and applications.
- Issue better patch and vulnerability technical publications. Publications should include more thorough analyses of the impact of vulnerabilities on unpatched systems as well as data on the environments and applications for which the patches were tested. Impact on other patches should also be addressed.
- Conduct independent security audits of the patch-development and deployment processes.
- Distribute a communication and mitigation plan, including how vulnerability/patch information will be relayed to the customer, for use in times of crisis.