Adobe
345 Park Avenue
San Jose, CA 95110
adobegr@adobe.com

April 8, 2013

VIA EMAIL
cyberframework@nist.gov

Diane Honeycutt
Division Secretary for Computer Security
National Institute of Standards and Technology (NIST)
U.S. Department of Commerce
100 Bureau Drive, Stop 8930
Gaithersburg, MD 20899

RE: Developing a Framework to Improve Critical Infrastructure Cybersecurity

Dear Ms. Honeycutt:

Adobe welcomes the opportunity to respond to your Request for Information (RFI) of February 26, 2013, "Developing a Framework to Improve Critical Infrastructure Cybersecurity." Adobe is a diversified software and services company, operating worldwide. Our principal focus is on digital media and digital marketing solutions. Our tools and services allow private-sector customers to create digital content, deploy it across media and devices, and then measure and optimize it over time. Adobe is also privileged to partner with government agencies to help them work more efficiently and cost-effectively. Adobe software is used to engage with citizens on multiple screens, manage workflows, secure information, and measure and analyze public engagement.

Adobe takes its responsibilities seriously to deliver high-quality software, developed using high security and privacy standards. Working together with other industry leaders, we make sure that when a threat or vulnerability arises, we provide customers with timely guidance and patches when needed as quickly as possible. We appreciate the opportunity that the RFI provides to discuss some of the processes and technologies that Adobe employs to develop its software and to provide tools that our customers can use to protect their data.

Current Risk Management Practices
[In response to NIST question 7 of the section]

Leading software companies utilize a variety of methods to secure the software development process. While these processes and implementations vary from one organization to another, the Adobe Secure Product Lifecycle (SPLC) is a rigorous set of more than 80 software development best practices, processes, and tools integrated into every stage of the product lifecycle and designed to help keep information safe and secure when customers use Adobe products.

Adobe
345 Park Avenue
San Jose, CA 95110
adobegr@adobe.com

Implemented by Adobe's dedicated security and incident response teams and complemented by continuous community engagement, the Adobe SPLC helps protect the security of information.

The main elements of the Adobe SPLC process include the following:

1. **Training and certification** provides the internal development teams with training and certification of the SPLC process and keeps them informed of the latest threats and approaches to software security.
2. **Requirements and planning** provides an overall health and risk assessment of a product or service and facilitate any necessary adjustments based on the current threat landscape.
3. **The design process** builds defenses against potential threats directly into the initial design of new products, as well as new features within existing products, and offers an opportunity to improve the security profile of existing features.
4. **Development and testing** embeds security best practices during development to help avoid coding issues and subjects code to rigorous internal and third-party tests using industry-leading testing frameworks and automated scanning tools.
5. **Staging and stabilization** helps ensure that the Adobe product or service is customer-ready and verifies code robustness, scalability, and resistance to attack in a production-like environment.
6. **The deployment process** minimizes risk of improper deployment through adherence to code handling processes and restricted access.
7. **The operations and monitoring process** monitors and logs traffic to help ensure maximum server availability and server health.
8. **Abuse, fraud, and incident response** helps ensure teams can respond quickly when incidents occur and guides interaction with security experts in the centralized Security Coordination Center to quickly and efficiently mitigate and resolve issues.

Along with following the SPLC, the Adobe Secure Software Engineering Team (ASSET) works with individual Adobe product security and operations teams to help achieve an appropriate level of security to protect our customers and their data. ASSET experts act as consultants to teams by advising on security best practices for clear, repeatable, consistent, and cross-functional processes for development, deployment, operations, and incident response. The team employs industry-standard benchmarks and reporting dashboards to constantly measure and convey progress in a variety of key areas. ASSET experts also maintain ties with the security community, exchanging information by collaborating with other organizations.

A key component of the ASSET program involves training, which enhances security knowledge throughout the company and improves the overall security of Adobe products. The ASSET team conducts ongoing security training within development teams across the company. Employees participating in the ASSET Certification Program earn points and attain different levels of certification by completing a variety of security projects. Employees begin training by learning basic security concepts (*e.g.* security in web-focused languages, such as Ruby on Rails and PhP), then move up to higher levels of training to gain an understanding of more complex security

Adobe
345 Park Avenue
San Jose, CA 95110
adobegr@adobe.com

topics and hands-on security coding experience. At the highest level, employees become security champions and experts within their development teams.

Specific Industry Practices
[In response to NIST questions 3, 11, and 12 of the section]

In general, a layered approach is what will drive improved security in the future. The idea is fairly basic – because any single defense may be flawed, a series of different security measures should be used to cover the gaps in the others' protective capabilities. Each of the items referenced in the RFI (*e.g.*, separation of business from operational systems, use of encryption and key management, monitoring and incident detection tools and capabilities, security engineering practices) can be used in conjunction with one another to develop a more secure system and protect information and communications technology (ICT) resources in ways the others may not be as capable.

Layered Security

Experts regard a layered approach to security as the best practice. Security in depth minimizes the chances that any single point of failure will result in the leak of information or the compromise of a system. Elements of a layered approach to security include protection at the data/document level, the application and OS levels, and finally at the network/perimeter level. Government should adopt layered security for its own use, and encourage its adoption by the private sector through voluntary means.

Adobe notes the U.S. Government has previously recognized that document digital rights management (DRM) is an important security control.[1] We further note that document-level security employing DRM has many uses to facilitate and secure both classified and unclassified information sharing, and the protection of personal information. Such technology is mature, flexible, robust, cost-effective, and available from a variety of U.S. software companies.

Thank you for giving Adobe the opportunity to provide comments on the development of the Framework to Improve Critical Infrastructure Cybersecurity. Should you have any questions or would like to discuss these comments, please contact me at adobegr@adobe.com.

Sincerely,

Brad Arkin
Senior Director, Security

[1] In the National Defense Authorization Act (NDAA) for FY2012, the Congress called on agencies under the Act to include "electronic auditing and reporting of unusual and unauthorized user activities and using data-loss-prevention and data-rights-management technology to prevent the unauthorized export of information from a network or to render such information unusable in the event of the unauthorized export of such information." (p. 388 H.R. 1540 National Defense Authorization Act for FY2012)