# IMPROVING SECURITY ACROSS THE SOFTWARE DEVELOPMENT LIFECYCLE

## TASK FORCE MISSION

At its core, the value of software is derived not only from its ability to increase productivity and efficiencies, but also from its resiliency to attack and always performing at needed levels during times of both crisis and normal operations. This task force's central thrust is towards establishing a world with robust software security, where users continue to benefit from software innovations. This is not an easy challenge and will take the persistent, combined efforts of industry, academia, government and others to make long-term progress. Only by increasing security-oriented efforts throughout the software development lifecycle can we achieve this key component of the President's National Strategy to Secure Cyberspace.

The task force's recommendations are a product of 4 smaller subgroups that parallel the multiple layers of the development lifecycle. Together these sub-groups have focused their mission on increasing software security through:

- enhancing the education and training of present and future developers to put security at the heart of software design and at the foundation of the development process [Education Subgroup];
- developing and sharing best practices to improve the quality of software, as well as the process so that systems are more resilient to attack [Software Process Subgroup];
- creating incentives that can create a culture of security awareness, and disincentives for malicious behavior [Incentives Subgroup];
- making the patching process simple, easy, and reliable [Patching Subgroup];

The task force as a whole also focused on how supporting basic research can increase the integrity, security, and reliability of software code development.

This task force has been led under the able leadership of its co-chairs Ron Moritz of Computer Associates, and Scott Charney of Microsoft. The Business Software Alliance has been secretariat for the task force.

## PROBLEM/CHALLENGE

Security is a serious problem and, if present trends continue, could be much worse in the future. No simple silver bullets will solve the software security problem. As a long-term multifaceted problem, it requires multiple solutions and the application of resources throughout the lifecycle. Improving software security and safeguarding the IT infrastructure is a research and education issue for universities; a skill, process, and incentives issue for producers; a requirements issue for customers; a quality and testing issue for providers; a maintenance and patching issue for IT administrators; an ease-of use issue for users; a configuration issue for installers; and an enforcement issue for governments.

## RECOMMENDATIONS

The ***Education Subgroup*** focused on present and future developers and recommends that 1) security become a core component of software development programs at the university level with sufficient resources to build the academic capacity to improve secure software development, and 2) supports the creation of an industry-led certificate program for security professionals and developers based on NICAB, and 3) supports improving security through software assurance centers of excellence. Specifically the group recommends:

- **Create A New Public-Private Effort To Build The Academic Educational And Research Capacity To Improve Secure Software Development.** This effort includes a set of recommendations for a university role in improving secure software development.

## IMPROVING SECURITY ACROSS THE SOFTWARE DEVELOPMENT LIFECYCLE

- **Create Software Security Certification Accreditation Program**. Support the creation of a certification and accreditation program for increasing security in software development.
- **Ensure that Software Assurance and other Information Technology Centers of Excellence include an information protection component.**

The ***Software Process Subgroup*** authored a report focused on best practices for putting security at the heart of the software design process. Principle recommendations listed below are focused on broadening use of the current most promising available practices for developing low defect secure software, to produce definitive studies that compare the relative effectiveness of available security practices, and to work within the software industry to achieve widespread use of effective security practices. The Subgroups principle recommendations are as follows:

**Principal Short-term Recommendations**

- Adopt software development processes that can measurably reduce software specification, design and implementation defects.
- Software producers should adopt practices for developing secure software.
- Software producers, where appropriate, should conduct measured trials of available approaches and publish their results.
- The Department of Homeland Security should support US-CERT, IT-ISAC, or other entities to work with software producers to determine the effectiveness of practices that reduce software security vulnerabilities.

**Principal Mid-term Recommendations**

- Establish a security verification and validation program to evaluate different software development processes and practices for effectiveness in producing secure software.
- Industry and the DHS establish measurable annual security goals for the principal components of the U.S. cyber infrastructure and track progress.

**Principal Long-Term Recommendations**

- Certify those processes demonstrated to be effective for producing secure software.
- Broaden the research into and the teaching of secure software processes and practices.

The ***Patching Subgroup*** defined steps to help make that the patching process simple, easy, and reliable. It developed a set of “Guiding Principles for Patch Management” for technology providers, critical infrastructure providers and independent software vendors. The group has recommended:

- **Adopting a “top-ten” list detailing industry best practices.** Patches should be well-tested, small, localized, reversible, and easy to install. Patches would also not require reboots, use consistent registration methods, include no new features, provide a consistent user experience, and support diverse deployment methods.

The ***Incentives SubGroup*** identified incentives to motivate development of more secure software, promote effective interaction between security researchers and software vendors, as well as disincentives for malicious behavior and cyber criminals. A new ‘Incentives Framework’ will document recommendations that policymakers, developers, companies and others can adopt to develop effective strategies and incentives for making software more secure, to include:

- Make the security of one's software a job performance factor;

## IMPROVING SECURITY ACROSS THE SOFTWARE DEVELOPMENT LIFECYCLE

- Develop industry awards for secure software development practices and end products;
- Create and actively distribute tools that illustrate secure software development techniques;
- DHS/NCSD should examine whether tailored government action is necessary to increase security across the software development lifecycle;
- Develop sample performance metrics for administrators/IT Departments that encourage effective action;
- Develop a multi-company program offering rewards for information leading to the conviction of cyber criminals;
- Track and measure, and then certify, effective development processes
- Create a program with government and industry support for Information Assurance/Computer Security faculty that provides a grant or reward for innovative educators in applicable fields for a fixed period of time;
- Create a National IT Security Certification Accreditation Program.

**NEXT STEPS**

- The Incentives sub-group will work to get commitments from the relevant actors to take the lead on implementing the programs and incentives outlined in the Sub Group's Framework.
- The process sub-group will work with major software vendors and key critical-infrastructure customer organizations to encourage and aid vendors in their adoption of the recommended low-defect, higher security-oriented practices and processes.

**CONCLUSIONS**

Overall, the task force has taken important steps forward in the long road toward implementing key components of the National Strategy to Secure Cyberspace. Establishing a lifecycle of robust security and ensuring that users continue to benefit from software innovations are critical goals that require continued progress. The challenges ahead cut across industries; governments and span the globe. And while improving research, education, the software development process, and patching processes will legitimately take time for the benefits to be achieved throughout the software lifecycle, the benefits are likely to be profound. Improving security throughout the software lifecycle can further increase the already dramatic economic and social benefits that software is already delivering.