

Securing Intel's External Online Presence

Overall, the Intel Secure External Presence program has effectively helped secure externally facing Intel-branded Web sites and solutions, resulting in a significant risk reduction for Intel's external presence.

Executive Overview

To protect Intel and its customers, Intel IT established a program that assesses, monitors, and enforces the security, privacy, and regulatory compliance of externally facing Intel-branded Web sites and online marketing programs.

Intel's business groups use hundreds of Web sites and third-party solutions—including social media platforms—to communicate and conduct business with customers and business partners. Collectively, these externally facing Intel-branded solutions are known as Intel's external presence.

Until 2006, these Web sites proliferated rapidly in response to business needs, without centralized oversight. Given this growth, we established the Intel Secure External Presence (ISEP) program to manage the risk associated with Intel's external presence.

The goals of ISEP, which is part of Intel's information security group, are to protect Intel's information assets and customers against threats such as loss of personal information and malware attacks, and to maintain compliance with laws, regulations, and standards. By achieving these goals, we also help to protect Intel's corporate image.

We improve protection and compliance by reviewing all planned new external presence projects and by monitoring existing Intel-branded Web sites. ISEP review and approval is mandatory for new externally facing online projects. We work with Intel business groups to review planned projects before launch, whether they are to be hosted within Intel

or by a third party. The ISEP process includes several key aspects:

- We make sure that we receive notification of new projects by working closely with business groups and other stakeholders within Intel. For example, we are notified when business groups request new Internet domain names or seek approval to install a new application in our externally facing environment.
- For each project, we work with the business group to review details of the planned approach to maintaining security and privacy compliance. We verify that the project includes any required mitigating controls before giving approval.
- A key to our success is an overarching governance board that provides enforcement powers and includes senior managers from multiple Intel stakeholder groups.

By January 2011, we had completed the ISEP security review process for more than 750 new projects. In addition, we conduct daily vulnerability scans on all of Intel's externally facing Web sites—more than 450—to maintain a high compliance level with a vulnerability assessment standard based on industry best practices. Overall, ISEP has effectively helped secure externally facing Intel-branded Web sites and solutions, resulting in a significant risk reduction for Intel's external presence.

Fred Leon
Program Manager, Intel IT

Contents

Executive Overview.....	1
Business Challenge	2
Intel Secure External Presence Program	2
Governance	2
ISEP Scope.....	3
ISEP Review Process.....	3
Managing External Suppliers.....	4
Monitoring and Securing Live Web Sites	5
Securing Virtual Events	5
Increasing Efficiency with Self-Certification of Low-Risk Projects.....	5
Results and Conclusion.....	5
Continuing Challenges	6
Key Learnings.....	6
Acronyms.....	6

IT@INTEL

The IT@Intel program connects IT professionals around the world with their peers inside our organization – sharing lessons learned, methods and strategies. Our goal is simple: Share Intel IT best practices that create business value and make IT a competitive advantage. Visit us today at www.intel.com/IT or contact your local Intel representative if you'd like to learn more.

BUSINESS CHALLENGE

Intel business groups use hundreds of externally facing Web sites to communicate and conduct business with consumers, enterprise customers, and external partners.

Until 2006 these Web sites proliferated rapidly, without central oversight, as each group identified specific business needs and deployed Web sites to meet those needs.

In early 2007 Intel's information security group created a team focused on centralizing and systematizing risk and security analysis for Intel's external presence. Key goals included creating a governance and review structure to monitor and improve the security, privacy, and legal compliance of existing and new external presence solutions. We needed to create a single repository documenting externally accessible Web sites and their ownership and remove sites that no longer provided business value.

The Intel Secure External Presence (ISEP) program evolved from this initial team. ISEP review is now an ongoing service that protects Intel and its customers by monitoring the ongoing security and policy compliance of externally facing solutions that are Intel-owned or Intel-branded.

INTEL SECURE EXTERNAL PRESENCE PROGRAM

The goals of ISEP are to protect Intel and its customers from unauthorized access to data and systems, and to maintain compliance with security, privacy, and regulatory requirements. By taking these preventative measures, we also help preserve Intel's brand and corporate identity.

We achieve these goals by working with Intel's business groups and other stakeholders to verify that externally facing online projects comply with Intel's security and privacy policies, and that they meet regulatory requirements. We review each project with the business group before launch. We also continue to monitor and audit Web sites after they go live.

The team began by establishing a schedule of regular meetings with internal Intel partners to identify potential security and privacy issues, and to develop corresponding solutions. These partners included representatives from Intel's sales and marketing groups, which generate many of the externally facing Web sites, as well as other stakeholders such as Intel's procurement and privacy groups. This also increased our visibility into new external presence solutions and projects. These meetings continue on a regular basis.

Governance

Intel instituted an overarching governance body, the External Presence Risk Review Board, to manage external-presence-related risks. The board provides the power to enforce any remedial actions that an ISEP review might identify. We also present information about external-presence-related security issues to the board, gaining support that enables us to implement corresponding recommendations.

The board includes senior leaders and decision makers from major stakeholders, including Intel's sales and marketing groups as well as Intel's information security organization. It ratifies and implements external presence security policies, initiatives, and risk-reduction activities.

ISEP Scope

Working with internal partners helped us to identify key focus areas, including:

- **Compliance with laws, directives, standards, and regulations.** These include the CAN-SPAM Act of 2003, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes–Oxley Act of 2002 (SOX), and the Children’s Online Privacy Protection Act of 1998 (COPPA); the European Union’s Data Protection Directive; export controls related to technology; payment card industry (PCI) standards; and e-Discovery regulations.
- **Privacy.** Protecting the personal information of Intel customers, business partners, and employees.
- **Security of Intel’s data.** Monitoring that classified data is not exposed to or accessed by unauthorized individuals.
- **Cyber-attacks.** Protecting Intel and its partners and customers against cyber-attacks, infections, and other cyber-crime activities.
- **Protecting Intel’s image.** Demonstrating that we are maintaining the highest ethical standards and Intel values.

For each external presence project, we assess security and privacy compliance across multiple project stages, ranging from application development to hosting, as shown in Figure 1.

ISEP Review Process

We made ISEP review a mandatory step in the approval process for all new externally facing online projects and programs—including those hosted within Intel IT and those hosted by a third-party. The steps in our review process are shown in Figure 2 and described in more detail below.

NOTIFICATION OF NEW EXTERNAL PRESENCE PROJECT

ISEP has forged links with other groups that are involved in implementing and approving

internally and externally hosted external presence solutions. These include Intel’s procurement, legal (including trademarks and branding), and Web marketing groups. For example, we partnered with Intel’s procurement group to trigger ISEP notification during the procurement process for externally hosted Web sites. We also trained Intel business group partners on the ISEP security review process and inserted ISEP requirements into the Web marketing group’s guidelines.

We receive notification of new external presence projects in a variety of ways:

- **Domain name requests.** ISEP is notified when a group requests a new Internet domain name; ISEP approval is required for all new Intel-owned domain names.
- **Internal hosting requests.** A cross-functional group conducts risk assessments for all externally facing solutions hosted in the Intel demilitarized zone (DMZ). This group must approve requests before the Intel IT operations group will implement the solution. ISEP is a member of this group and has a dedicated person assigned to review DMZ-based solutions as well as lead security governance in this space.
- **Trademark and branding clearance requests.** We are automatically copied on clearance form submissions to Intel’s trademark and branding group.
- **Procurement requests for externally hosted solutions.** We work with Intel’s procurement group so that ISEP is notified when sourcing providers for externally hosted projects. ISEP notification is triggered during the procurement process, and we have added security and privacy information into purchasing tools, templates, and processes—verifying suppliers are informed of our requirements and that the information is incorporated into contracts. In addition, ISEP is a member of the Intel board that reviews and approves new suppliers.

- **Existing business partners.** Our existing business group partners are familiar with the ISEP process and requirements, and often notify us of new projects as a matter of course.

ASSIGN ISEP ENGAGEMENT MANAGER

Once we receive notification of a new project, we assign an ISEP engagement manager, who schedules a discovery meeting with the business group planning the external presence solution.

CONDUCT DISCOVERY MEETING

During the discovery meeting, we gather information including:

- A project overview
- Details of the data collected, exposed, or used
- Information about the Web site developer and the planned hosting arrangement
- Planned security controls

This information enables us to identify the security and privacy requirements for the project.

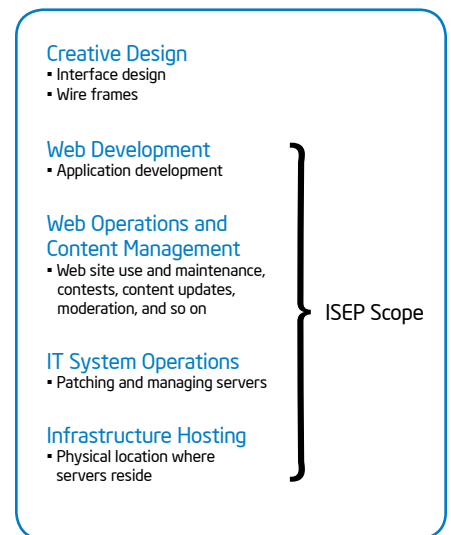


Figure 1. New external presence projects at Intel undergo a series of reviews as part of the Intel Secure External Presence (ISEP) program.

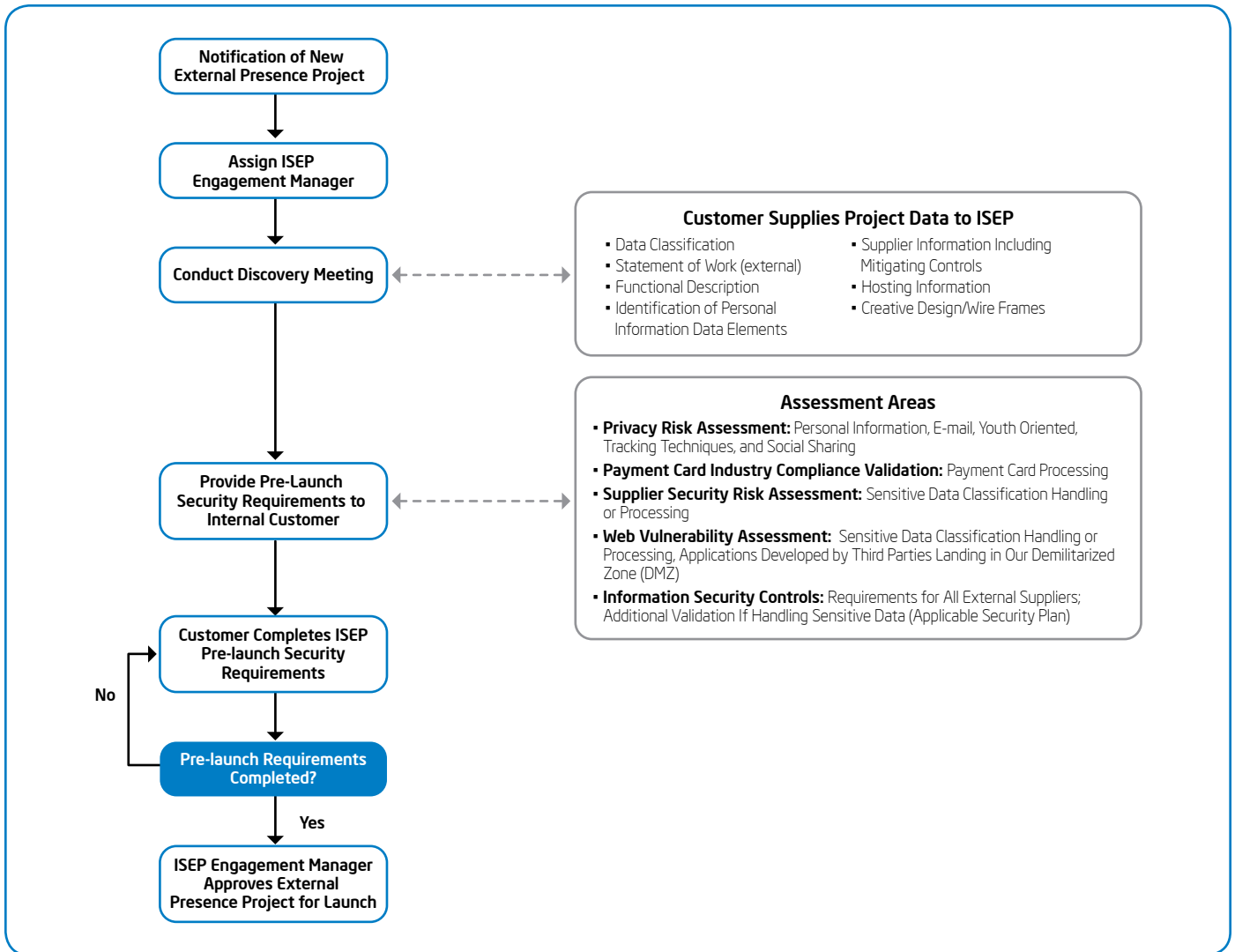


Figure 2. The Intel Secure External Presence (ISEP) program mandates a series of tasks prior to the launch of externally facing Web sites to help protect corporate and customer data.

PROVIDE PRE-LAUNCH SECURITY REQUIREMENTS TO INTERNAL CUSTOMER

Following the discovery meeting, we create a list of security and privacy requirements that we share with the business group and will need to check before approving the project. The requirements vary depending on factors such as the classification of the data exposed, collected, or used and where the solution will be hosted, as shown on the right in Figure 2.

REVIEW AND APPROVE

We review the project's security and privacy controls in the relevant areas. This includes verification of planned mitigations for any risks—such as encryption for sensitive data. Once we have approved the project, we inform the customer and any other Intel groups involved in approving the project.

Managing External Suppliers

We provide a document to suppliers that develop, host, or support an Intel-owned external presence solution explaining both our general expectations and specific security requirements for handling data and security incidents. We append this document to all relevant contracts and review it with suppliers to verify compliance.

General supplier expectations include:

- Identifying potential threats and vulnerabilities through ongoing risk analysis, and implementing effective controls.
- Having a specific resource that is accountable for managing security.
- Suppliers are responsible for sub-contractor compliance with Intel's security requirements and expectations.

Specific requirements include reporting to Intel any security event involving or impacting Intel data or an Intel Web site. For events that involve Intel classified data, branding, or other specific proprietary information, the reporting must occur within a specified timeframe.

MAINTAINING THE APPROVED SUPPLIER LIST

We partner with Intel's procurement and Web marketing groups to implement and enforce an approved supplier list. This identifies Web development and hosting suppliers who are approved to host Intel-branded Web sites.

As Intel's business needs change, we will continue to work with procurement to modify the approved supplier list. Maintaining a manageable number of suppliers is an ongoing challenge, because many Intel solution owners have preferred suppliers.

Monitoring and Securing Live Web Sites

In addition to reviewing new projects before implementation, we monitor and enforce the security and privacy compliance of existing Web sites.

DAILY VULNERABILITY SCANNING

We implemented a daily application vulnerability scanning process for Intel-owned externally accessible Web sites. This process, built on a third-party solution, checks all Web sites for known security vulnerabilities.

We established an enforcement process to verify that all significant vulnerabilities discovered are remediated within the required timeframe. Characteristics of this process include:

- Notification and management escalation is based on the severity of the risk. For example, discovery of a high-risk vulnerability results in notification of the supplier and Intel business group owner.
- We enforce a tiered remediation timeline based on the severity of the risk. The greater the risk, the more quickly it must be remediated.
- We apply the same enforcement standards to both internally and externally hosted sites.

We communicate our security metrics and remediation progress in regular reports to partner groups and stakeholders. This helps our procurement group identify at-risk suppliers and their responsiveness to remediating vulnerabilities found.

We also instituted an audit process to validate that live sites contain any required privacy, legal, and data protection notifications.

We implemented an identification process to find any rogue Web sites launched without ISEP-required checks. When we identify sites through this process, we verify that they include the appropriate controls required to protect Intel and its customers.

Securing Virtual Events

ISEP partnered with other Intel IT teams to develop and implement a secure virtual event capability that can be used by all Intel business groups. We helped improve the implementation of the appropriate security controls to protect the information collected and stored. We developed a standard set of security requirements that streamline review and approval for typical small virtual events across Intel.

Increasing Efficiency with Self-Certification of Low-Risk Projects

ISEP review is a required step in all new external presence projects, so it is essential to make the review process as efficient as possible. By applying Lean Six Sigma* methodology to analyze our process efficiency, we identified a way to automate review of low-risk projects. This will help business groups launch low-risk Web sites quickly, while allowing us to focus resources on higher-risk projects.

To automate this process, we developed a portal that will enable customers to self-certify low-risk projects; based on their answers to a set of questions, the project may be categorized as low-risk and may be automatically approved. ISEP stores a copy of the customer-provided information in case it is needed in the future for audit or other purposes.

RESULTS AND CONCLUSION

We have successfully developed ISEP review into an ongoing service that protects Intel and its customers by helping improve the ongoing security and policy compliance of externally facing solutions that are Intel-owned or Intel-branded. As the program has matured, we have experienced a significant reduction in risk for Intel's external presence.

By January 2011, we had completed the ISEP security review process for more than 750 new projects. In addition, we conduct daily vulnerability scans on all of our externally facing Web sites—more than 450 in total—to maintain a high compliance level against a

vulnerability assessment standard based on industry best practices. Overall, ISEP has effectively helped secure Intel-branded externally facing Web sites and solutions, resulting in a significant reduction in risk for Intel's external presence.

Continuing Challenges

Though the ISEP program has been effective, challenges remain. These include:

- With the growth of social media platforms, business groups increasingly want to use them to communicate; we therefore provide guidance to employees regarding acceptable use.
- Maintaining a complete, accurate inventory of all external presence assets. This includes tracking changes in Web site ownership as employees move to new positions or leave the organization. It is important that the relevant business groups take responsibility for maintaining and updating information in this inventory.
- Detecting changes to older Web sites, to assess the security and privacy ramifications.
- Managing and enforcing the use of approved suppliers.
- Keeping up with demand and knowing where to focus our ISEP reviews, as Intel business groups continue to expand their online presence.

Key Learnings

Our experience in applying the ISEP review process during the past four years has taught us a number of valuable lessons.

- Simplify the security engagement and review process for the customer. If it's not simple, people may not use it.
- Review and classify all data exposed, collected, or used, especially personal information.
- Make sure cross-organizational governance is in place to support enforcement actions.
- Verify that Web site owners know they are accountable for the solutions they deploy. This includes responsibility for policy compliance, life cycle management, and supplier management.
- Include appropriate security and privacy language in all supplier contracts.
- Deploy detective controls that continually monitor externally facing solutions for compliance and security.
- Hold internal and external Web site owners to the same security standard.
- Implement an enforcement process that is clearly documented and supported by senior management.
- Collect metrics to demonstrate efficiency—such as progress in remediating vulnerabilities and the time required for the review process. This helps us be efficient and effective.
- Build a single repository to manage the life cycle of all externally facing Web sites.

CONTRIBUTORS

Brently Davis
Kurt M. Nelson

ACRONYMS

COPPA	Children's Online Privacy Protection Act of 1998
DMZ	demilitarized zone
HIPAA	Health Insurance Portability and Accountability Act of 1996
ISEP	Intel Secure External Presence program
PCI	payment card industry
SOX	Sarbanes–Oxley Act of 2002

For more information on Intel IT best practices, visit www.intel.com/it.


This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any patent, copyright, or other intellectual property rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2011 Intel Corporation. All rights reserved.

Printed in USA
0511/IPKA/KC/PDF

 Please Recycle
324595-001US

