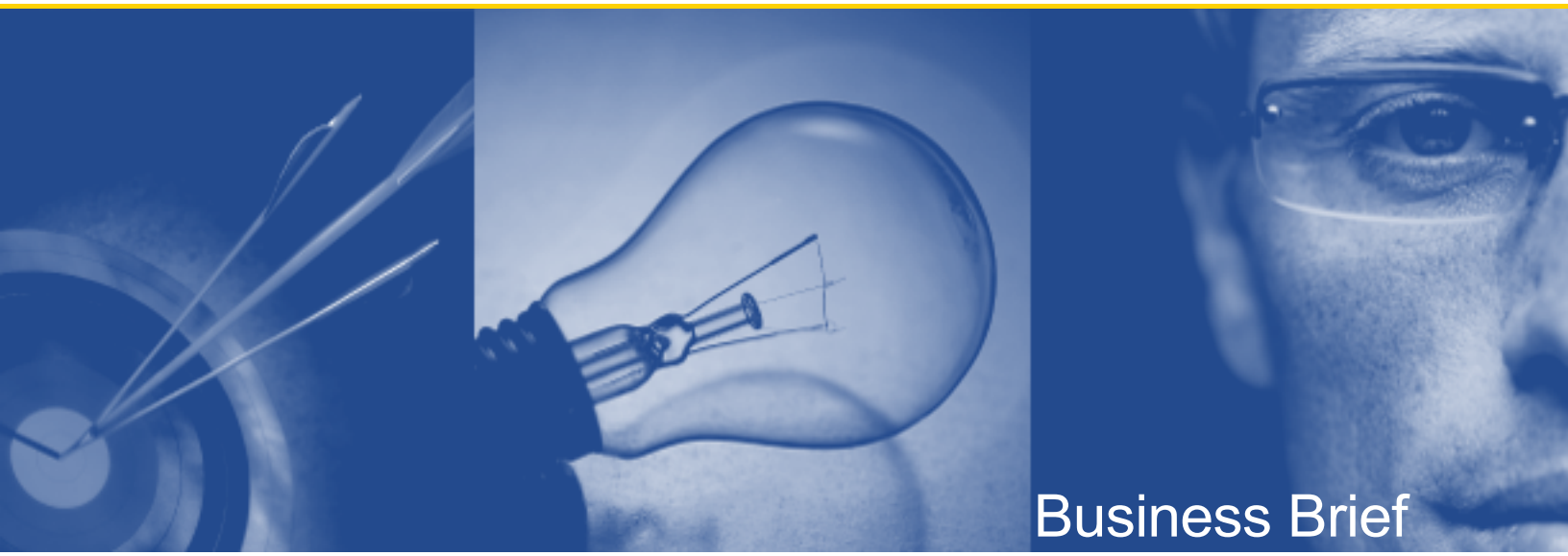
QUEST SOFTWARE®

Cybersecurity Frequently Asked Questions

How Quest Solutions Can Provide Protection from Internal and External Threats

Written by
Quest Software, Inc.



WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters:
5 Polaris Way
Aliso Viejo, CA 92656
e-mail: info@quest.com

Please refer to our Web site (www.quest.com) for regional and international office information.

Updated—August 2009

INTRODUCTION

This brief provides Quest Software's responses to the most frequently asked questions about the security of our products and their compliance with federal guidelines and regulations. It also summarizes Quest solutions that can help achieve FISMA compliance by mapping them to corresponding FISMA controls.

1. What are Quest's R&D security procedures?

Quest 's security and compliance architect performs security assessments of all Quest products. These assessments follow a detailed checklist and are cross-referenced against the security categories specified by US NIST in publication 800-53. This assessment is provided to customers upon request to review the security features of the product.

The security and compliance architect has developed the following security best practices for Quest R&D:

- Complete security assessments of all Quest products, as described above
- Develop code samples and architecture templates that cover common security operations
- Train and mentor developers to increase awareness of code security issues
- Monitor US-Cert for vulnerabilities in third-party components used by Quest products. This process ensures that security patches to these components are applied in a timely manner
- Sign all distributed software with digital code to prevent tampering
- Review the use of cryptography in Quest products with guide development teams
- Ensure that all teams are aware of and meet compliance standards such as Federal Desktop Core Configuration (FDCC), FIPS 140-2, FIPS 201, Common Criteria, IPv6

Quest's security and compliance architect regularly meets with government officials, participates in cyber and information assurance forums and advises the Quest product development groups.

2. Are Quest products FISMA certified?

A product cannot be FISMA (Federal Information Security Management Act of 2002) certified. FISMA only provides guidance and instructions that government agencies must follow to maintain a high level of security within their systems and networks.

When Quest performs security assessments on a product, we map its security features to NIST 800-53, the basis of most FISMA controls. This allows a government agency to evaluate how its adherence to FISMA is affected by the installation of a Quest product.

3. Do any Quest products meet ISO27001 standards?

An organization can be ISO 27001 certified. It is not a standard for individual products. Quest is currently not ISO 27001 certified.

However, Quest does have its own internal security best practices, most notably the security and compliance assessments of our products. The assessment documents clearly outline relevant security information and address most agencies' security concerns.

4. How does Quest meet Common Criteria, NIAP, and NIST requirements?

The Department of Defense (DOD) and the National Institute of Standards and Technology (NIST) formed the National Information Assurance Partnership (NIAP) to implement the policies established by the July 1990 National Security Directive No. 42. This policy directive pertains to the acquisition and use of commercial off-the-shelf (COTS) information assurance (IA), or IA-enabled products that are used on systems that enter, process, store, display or transmit national security information.

An IA product is defined as an IT product or technology is primarily used to provide security and a layered defense against non-authorized and malicious penetrations of information systems or networks, as well as correct known vulnerabilities. An IA-enabled product is a product or technology that does not directly provide security, but includes security services as an associated feature of its intended operating capabilities. To meet the requirements of National Security Telecommunications and Information Systems Security Policy (NSTISSP) 11, acquired IA-enabled products must be evaluated by the government to determine if they are going to be used to perform one of the security services—availability, integrity, confidentiality, authentication, or non-repudiation. Quest understands that an IA-enabled product must be evaluated according to how the particular product will be used within the government's system architecture.

Quest has a long history of working with the federal government and is committed to achieving government security standards, including the requirements of Common Criteria, FIB PUBS 140/201, FISMA, and other information assurance processes and validations. We use only the best security practices to secure the operating system, handle sensitive data, protect network communications, and limit access, using FIPS 140-2 compliant technologies.

Quest's product security documentation can help agencies determine if our products meet specific security requirements. Our technical support team can provide you with any needed documentation and has worked with many customers to address their NIAP, Common Criteria, FISMA, FIPS, C & A requirements.

URL: http://www.quest.com/public-sector/common-criteria.aspx

5. Are Quest products certified and accredited (C & A)?

Software products cannot be certified and accredited (C & A); only federal networks and environments can be certified and accredited. When Quest delivers a commercial off-the-shelf (COTS) product, we assume that it is for deployment/installation on an existing C & A environment. The Quest solution is considered an upgrade to the existing certified environment, and should require only agency environment scanning or testing. To eliminate vulnerability concerns, Quest can provide a product trial to your security / IT administrators to execute vulnerability scans in a test and/or production environment. This test can also be used to determine configuration requirements. We will work with you and your security staff to prepare this technology for your environment and to ensure that it meets your requirements.

6. How does Quest meet FIPS 140-2 requirements?

Whenever possible, Quest Software is committed to product security and assurance and plans on using FIPS 140-2-approved cryptographic modules in its products. Where this is not possible, we will ensure that any Quest product with cryptography supports FIPS 140-2-approved algorithms, including symmetric and asymmetric encryption, hashing, keyed hashing, message authentication, and random number generation.

We review the use of cryptographic algorithms in our products during our security and compliance reviews. Where we find that a product does not support FIPS 140-2 compliant algorithms for its cryptographic operations, we will schedule the addition of the appropriate cryptographic algorithms in the next major product release or sooner.

We will continue to discuss cryptography standards and processes with our U.S. federal government customers.

URL: http://www.quest.com/public-sector/fips-140-2.aspx

7. Are Quest products compatible with the migration to IPv6?

Quest supports the U.S. government's migration to IPv6.

Most of our products delegate networking to lower levels of the stack and are IP addressing-scheme agnostic. We expect these products to work on an IPv6 network without modification. To ensure this, we have set up an IPv6 environment for product testing.

To support IPv6, Quest has started to revise the way that a small number of our products handle IP addresses in order to accommodate the new 128-bit ones. However, URL: http://www.quest.com/public-sector/ipv6.aspx

8. Are Quest products FDCC certified?

Quest has received numerous Federal Desktop Core Configuration (FDCC) certifications for some products. We have an established FDCC testing environment within our R&D organization and use National Institute of Standards and Technology (NIST) certified Security Content Automation Protocol (SCAP) vulnerability scanning and certification technologies. We will evaluate subsequent product releases against the latest FDCC baseline, and document any known exceptions. Development plans will address future exception.

URL: http://www.quest.com/public-sector/fdcc.aspx

9. Are any Quest products FDCC compliant?

Yes. You can find a subset of our FDCC-compliant products and their accompanying certification letters here:

http://www.quest.com/public-sector/fdcc.aspx

10. Are you certified to run on the Air Force or DOD network?

Quest products are used throughout the DOD on accredited and certified networks. Please check with your chief information security officers to determine the policies and procedures for introducing a new Quest product.

11. What are Quest's cybersecurity solutions and how do they prevent attacks?

The following table summarizes the key FISMA controls for preventing and responding to infrastructure attacks and lists the Quest solutions that can help achieve FISMA compliance:

CONTROL	QUEST SOLUTIONS
2: Inventory of authorized and unauthorized software; enforcement of white lists of authorized software	• Quest Management Xtensions – Configuration Manager 2007 Edition • Policy Authority for Unified Communications • Reporter • SecurityManager
3: Secure configurations for hardware and software for which such configurations are available.	• Desktop Authority • vWorkspace • SecurityManager
5: Boundary defense	• Policy Authority for Unified Communications • Quest Defender
6: Maintenance, monitoring, and analysis of complete audit logs	• InTrust • InTrust Plug-In for Active Directory • InTrust Plug-In for Exchange • InTrust Plug-In for File Access • ChangeAuditor for Active Directory • ChangeAuditor for Exchange • ChangeAuditor for File Systems
8: Controlled use of administrative privileges	• ActiveRoles Server • InTrust • Quest Defender • Privilege Manager for Unix • SecurityManager

CONTROL	QUEST SOLUTIONS
9: Controlled access based on need to know	• Authentication Services • ActiveRoles Server • Access Manager • Privilege Manager for Unix • Policy Authority for Unified Communications
11: Dormant account monitoring and control	• ActiveRoles Server • Authentication Services • Reporter • MessageStats • Access Manager • InTrust • InTrust Plug-In for Active Directory • InTrust Plug-In for Exchange • InTrust Plug-In for File Access
13: Limitation and control of ports, protocols, and services	• SecurityManager
15: Data leakage protection	• InTrust • InTrust Plug-In for File Access • Archive Manager • Policy Authority for Unified Communications
18: Incident response capability	• InTrust
19: Disaster recovery capability	• Recovery Manager for Active Directory • Recovery Manager for Exchange • Recovery Manager for SharePoint • LiteSpeed • SharePlex for Oracle • Policy Authority for Unified Communications • vReplicator • vRanger Pro

CONCLUSION

Quest believes that the nation's approach to cybersecurity over the past 15 years has failed to keep pace with the threat. We agree with the following statement from the Commission on Cybersecurity for the 44th Presidency, "America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration."[1]

State and federal agency IT executives face three critical cybersecurity challenges:

- Government agencies are prime targets for cybersecurity crime. It is vital that they close all gaps in their IT systems to ensure 24x7 security and protection.
- The president has mandated that federal stimulus money be spent on cybersecurity initiatives, yet it is not clear exactly which initiatives are cybersecurity-worthy.
- Any purchase or deployment under this budget guideline must clearly correlate cybersecurity-related improvements to the amount of dollars spent.

Cybersecurity attacks are real, and government agencies are prime targets. Quest solutions for cybersecurity meet government mandates for providing safe, reliable and resilient IT systems. Quest provides smart security technologies that enable agencies to protect our nation's information assets from security threats—both internal and external.

1 Report of the Commission on Cybersecurity for the 44th Presidency, December 2008

ABOUT QUEST SOFTWARE, INC.

Now more than ever, organizations need to work smart and improve efficiency. Quest Software creates and supports systems management products—helping our customers solve everyday IT challenges faster and easier. Visit www.quest.com for more information.

Contacting Quest Software

Phone:	949.754.8000 (United States and Canada)
Email:	info@quest.com
Mail:	Quest Software, Inc. World Headquarters 5 Polaris Way Aliso Viejo, CA 92656 USA
Web site	www.quest.com

Please refer to our Web site for regional and international office information.

Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf