UNITED STATES DEPARTMENT OF COMMERCE
Office of the General Counsel
Washington, D.C. 20230

JAN 30 2004

Mr. Chris Hoofnagle
Associate Director
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Dear Mr. Hoonagle:

This is in response to your Freedom of Information Act (5 U.S.C. § 552) (FOIA) appeal for information withheld in the fourth interim response to your request with the National Institute of Standards and Technology (NIST) for all agency records related to "Trusted Computing," or related technology that were created or came under agency control since January 1, 2002.

By letter dated July 18, 2003, you requested this information. By letter dated December 19, 2003, Sharon E. Bisco, NIST FOIA Officer, informed you, in a fourth interim response to your request, that two documents were being provided to you and that one 89-page document was being withheld pursuant to 5 U.S.C. § 552 (b)(4).

In your appeal, you state that NIST did not adequately explain the content of the withheld material and that the agency is under an obligation to segregate and release portions that do not contain (b)(4) information. You also say that material related to "Trusted Computing" should generally not be protected from disclosure because the subject matter concerns an open computer architecture that can be employed on any operating system, and since Microsoft has described the technology as designed for openness. Your appeal is granted in part.

We found that the information at issue was not described completely in the response to your request. Instead of one 89-page document, the information in fact consists of nine separate documents, totaling 67 pages. Duplicate pages were included in the page count. Six of these nine documents are being released to you in their entirety. Portions of two documents are being withheld pursuant to FOIA exemption (b)(4) and portions of one document are being withheld pursuant to FOIA exemption (b)(6).

The (b)(4) information is contained in two unsigned documents between NIST and Microsoft, a U.S. Government Security Program Source Code Agreement (GSP Agreement) and a Government Security Program Authorization. The withheld information consists of confidential commercial information pertaining to proposed terms of the agreement. This information is exempt from disclosure pursuant to FOIA exemption (b)(4), which protects from disclosure

commercial or financial information which is privileged or confidential. It does not consist of any transparent technology, but instead constitutes commercial terms proposed by Microsoft. Commercial or financial information is considered "confidential" for purposes of the exemption if disclosure is likely to impair the Government's ability to obtain necessary information in the future, if it is likely to cause substantial harm to the competitive position of the person from whom the information was obtained, or if it will significantly harm a strong Government interest. National Parks & Conservation Association v. Morton, 498 F.2d 765, 770, 770 n. 17 (D.C. Cir. 1974); Comstock International, Inc. v. Export-Import Bank of the United States, 464 F. Supp. 804 (D.D.C. 1979); 9 to 5 Organization for Women Office Workers v. Board of Governors of the Federal Reserve, 721 F.2d 1 (1st Cir. 1983).

Personal information (including a cell phone number) have been redacted from one document pursuant to FOIA exemption (b)(6), which protects personal privacy interests and exempts from disclosure all information about individuals in "personnel and medical files and similar files" if disclosure "would constitute a clearly unwarranted invasion of personal privacy." The term "similar files" has been interpreted broadly to apply to almost any information which applies to a particular individual. Department of State v. Washington Post Co., 456 U.S. 595, 599-603 (1982).

All releasable material has been segregated from protected information and released to you. This is the final decision of the Department of Commerce. You have the right to obtain a judicial review of this response to your FOIA appeal as provided in 5 U.S.C. § 552(a)(4)(B).

Sincerely,

Barbara S. Fredericks
Assistant General Counsel for Administration

Enclosures

Microsoft's Government Security Program

Monday, March 17, 2003

Introduction

- Government Security Program (GSP)
- Provides national governments and international organizations with access to Windows source code and other technical information
- Part of MS Trustworthy Computing and Shared Source initiatives

GSP Source Code Agreement

- Three-year relationship
- Access to source code via the MSDN Code Center Premium
- Apply to employees and approved agency contractors
- Use a smart card to access the code
- Review the code
- Contact Microsoft to ask additional questions or documentation
- Visit Microsoft to review their source-code development, testing and deployment processes

Benefits

- Secured online access to Windows 2000, XP , 2003 and CE source code using a smart card
- Conduct security audits
- Improved troubleshooting
- Access to cryptographic code
- Communication and collaboration with Microsoft Security professionals
- Opportunity to visit Microsoft development facilities

Roles and Responsibilities - I

- A single national government division or authority as the sponsoring agency within each participating nation
- Three-year GSP Code Agreement
- Conduct the security review on behalf of the national government
- Lead agency may authorize other government agencies access to the resource for project-specific source code, including authorized agency employees and contractors/consultants
- Lead agency sign a three-year Source Code Agreement which is the framework and an annual Source Code Authorization which is the license grant with Microsoft

Roles and Responsibilities - II

- Sponsored agencies are authorized by the lead agency to access the source code
- Sponsored agencies sign sign an authorization with a lead agency and Microsoft
- Once a sponsored agency has be authorized, it has a direct relationship with Microsoft
- Agency employees are listed by the government in the Code Center Premium smart card fulfillment form
- Contractor/consultant must sign an Additional Personal Exhibit with the agency and Microsoft

GSP lifecycle - I

- Sign Agreement and Authorization
  - Lead Agency
    - Three-year GSP Source Code Agreement
    - Annual GSP authorization (project-specific source-code access license)
  - Sponsored Agency
    - Nominated by the lead agency
    - Sign an Authorization with Microsoft and lead agency
    - Identify and agree to the scope of the authorization
    - Sponsor agency works directly with Microsoft

GSP lifecycle - II

- Obtain access to GSP Code Center Premium website
  - Microsoft sends the agency contact a welcome letter and account request form
  - Primary contact fills out the account request form for each person who requires access to the source code
  - Once the request form has been processed, Microsoft sends the Welcome Package 1 which includes the smart cards
  - Welcome Package 2 which includes the smart card reader and software is sent
  - Once the smart cards have been distributed, the primary contact or individual user sends an email requesting a PIN
  - Once the PIN is received, the user can access the Code Center Premium for GSP

GSP lifecycle - III

- Review Code
  - Participant may view and search the code
  - Physically take place in authorized government facilities specified in the GSP Authorization
  - Only authorized personnel can review the code
  - May not share any details or imply the contents of the source code
  - May not share specific architectural design or refer to specific files X, Y, and Z

GSP lifecycle - IV

- Reporting security vulnerabilities during review
  - Send email to gspsec@microsoft.com
  - Include the following information:
    - Contact information
    - Computer information
    - Context for report
    - Affected product
    - Vulnerability information (step-by-step)
- Microsoft respond by reviewing the report, reproducing the vulnerability, developing/testing fix and documentation, distributing back to the customers, and incorporating the lessons learned in development practices

GSP lifecycle - V

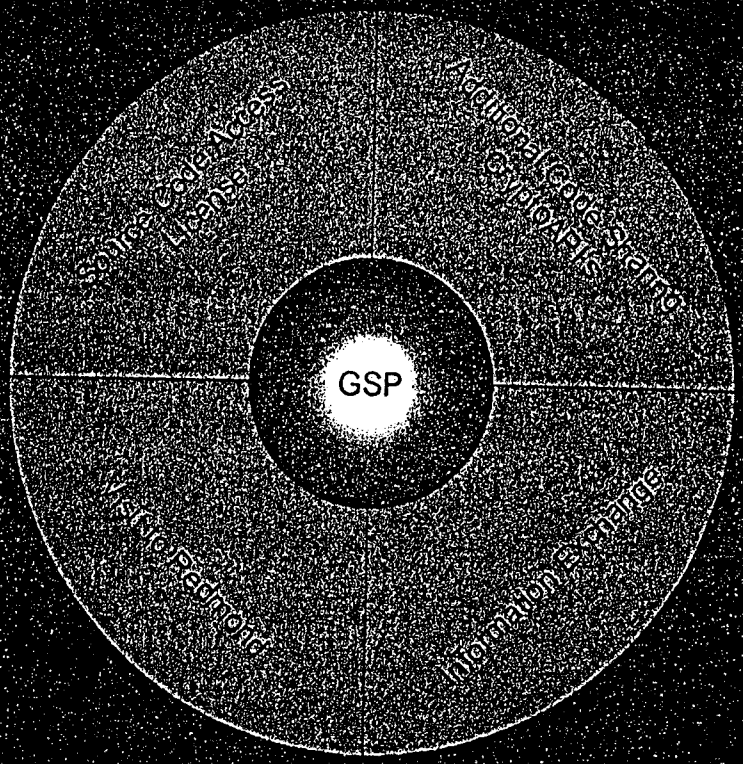
- Microsoft can arrange for source code workshop on location or at Microsoft campus
- Participants may opt to visit Microsoft development facilities once they have outlined specific projects and objectives prior to arrival
- Participants may request additional information by sending email to gspteam@microsoft.com
- Authorization are valid for one year and renew annual if no change is made
- Participants continue with the review
- At the end, agencies must return or destroy all copies of source code and provide Microsoft with a letter stating this fact

Government Security Program: Program and Agreement Overview

Sean Finnegan
Federal Security Program Manager
November 21, 2002

GSP at a Glance

- The Microsoft Government Security Program (GSP) is designed to provide national governments the information they need to be confident in the security of the Microsoft Windows platform.
- The GSP is about:
  - Transparency through free access to source code of Windows 2000, Windows XP, Windows .Net Server, and Windows CE
  - Information exchange and opportunity to visit Microsoft campus in Redmond to discuss security
  - Partnership through increased interaction, trust and relationship building



Source Code Access and Information Exchange

- License for Source Code Access:
  - No fee source code access to "lead agency" for security review
  - Lead agency can sponsor other governmental agencies with annual project-specific source code access authorizations
  - Access to agency employees and MS approved contractors
  - Provide smart-card based online source code access through MSDN Code Center Premium.
  - Provide Microsoft cryptographic code implementation in source code form (subject to US export approval)
- Expanded information and technical disclosure to help governments build secure infrastructure
- Demonstrate platform richness by providing engineering-level information on Windows architectural design as it relates to security
- Make available Crypto Service Provider developer kit for governments interested in developing and implementing their own cryptographic module

Mutual Trust and Partnership Building

- The GSP is based on mutual trust:
  - Trust in accessing source code
  - Trust in information exchange and feedback
- Invitation for Partnership Visit for one to two weeks in Redmond:
  - Agency submits proposal outlining specific goals and objectives in coming to Redmond prior to arrival
  - Goal is to give Agency the opportunity to review source code, see how Windows is built, meet with cross-section of people
- Visit gives Microsoft the opportunity to get valuable feedback
- Opportunity for cooperation on projects identified in GSP Authorization provides framework for building trust and partnership
- GSP as basis for future technical partnerships enabling the government to design, build and deploy secure infrastructure

GSP Source Code Agreement: Embodying the GSP Value Proposition

GSP Value Proposition:

"The Microsoft Government Security Program is designed to provide national governments the information they need to be confident in the security of the Microsoft Windows platform."

- The GSP Agreement is the source code license that allows Microsoft to extend the benefits of the GSP to the government and give the government access to the source code.
- The GSP Agreement is meant to be relatively simple, even-handed and uniform.
- It provides a balance between giving each GSP participant the full benefit of the program and protecting Microsoft's most valuable intellectual property assets.
- The documentation is standardized for consistent application across the world yet is flexible enough to accommodate different requirements in access to and usage of code.
- The GSP Agreement is the basis for a 3 year relationship with a governmental agency and facilitates future cooperation.
- The GSP Authorization identifies mutually agreed upon security related projects

The Paper Trail

Legal framework for relationship

- Between Microsoft and one Agency representing Government
- Effective when at least one Authorization is signed
- Contains license grant and limitations
- Terms apply to employees and contractors

GSP Source Code License Agreement

- Standard document that provides base-line terms

- Smartcard access through Code Center Premium
- Provides for trade secret protection
- Invites feedback
- Three year term

GSP Autho-rization

- Applies (unless project requires it)
- One year term (renewable)
- Authorization Specifies:
  - License granted
  - Purpose of grant
  - Products involved
  - Govt. facilities

GSP Summary

- A no-fee source code license for a lead government agency providing access to the Windows Premium Source Code Kit through MSDN Code Center Premium for purposes of security review
- Technical information and support to enable understanding of Windows security and enhance ability to implement Windows security technology
- A framework for future collaborative IT security efforts with the governments
- Requires entering into GSP Source Code Agreement and at least one GSP Authorization
- Structured so that one lead Agency enters into agreement and conducts security review on behalf of government or sponsors other governmental agencies for specific Authorizations
- We welcome your participation!