X-Sender: grance@email.nist.gov
X-Mailer: QUALCOMM Windows Eudora Version 5.1
Date: Fri, 06 Dec 2002 14:47:57 -0500
To: grance@erols.com
From: Timothy Grance <grance@nist.gov>
Subject: Fwd: MS source code

X-Sieve: CMU Sieve 2.2
X-Sender: souppaya@csmes.ncsl.nist.gov
X-Mailer: QUALCOMM Windows Eudora Version 5.1
Date: Fri, 29 Nov 2002 13:46:29 -0500
To: grance <grance@nist.gov>
From: Murugiah Souppaya <souppaya@nist.gov>
Subject: MS source code

Tim,

Here are my comments regarding MS Source Code.

1. NIST and their collaborators, i.e. CSD, ITL, other labs, Govt. agencies, contractors, etc, will be able to have access to all MS source code ranging from the OS, Applications server, middle-ware, crypto code, mobile devices etc.
2. NIST can build a close relationship with MS technical team where direct access to the MS experts will be readily available. This will reduce the amount of time that is usually wasted while trying to find the appropriate individuals who are intimate with the MS technology.
3. NIST can produce guidance documents in a timely manner and even influence default MS installations before they are being shipped.
4. NIST may be criticized for working to closely with MS but this may lead other companies to share their source code.

I have made these observations based on the following facts:
1. NIST does not manage or maintain the code repository server. The source codes are stored on a secure MS server and infrastructure.
2. If NIST accepts to participate in the program, it would only be for a predetermined period of time, i.e. 1 to.3 years.

Murugiah

X-Sender: grance@email.nist.gov
X-Mailer: QUALCOMM Windows Eudora Version 5.1
Date: Fri, 06 Dec 2002 14:47:43 -0500
To: grance@erols.com
From: Timothy Grance <grance@nist.gov>
Subject: Fwd: access to MS source

X-Sieve: CMU Sieve 2.2
X-Sender: jansen@email.nist.gov
X-Mailer: QUALCOMM Windows Eudora Version 4.3.2
Date: Fri, 29 Nov 2002 12:10:40 -0500
To: timothy Grance <grance@nist.gov>
From: "W. Jansen" <wjansen@nist.gov>
Subject: access to MS source

From time-to-time access to the source code of MS products would be useful. For example, when we looked at Windows CE/Pocket PC for our work on multi-factor authentication on PDAs, we were stymied because of lack of publicly available documentation on the available internal programming interfaces supported by the OS. Without source code to review, the only alternative available is to treat the implementation as a black box. In speaking with manufacturers of security mechanisms for the Pocket PC environment, they expressed much frustration with having to apply this sort of trial-and-error approach.

Besides project implementation work, access to product source code might prove useful when preparing guidance to agencies, especially in more recent documents where we have tried to provide highly-detailed software configuration information. The only drawback I see is having to put in place adequate safeguards and procedures to protect proprietary source code adequately from within our division.

Microsoft's Government Security Program

Participant Procedure Guide

Microsoft Confidential

Microsoft Corporation
Published: March 2003

Abstract

National governments and international organizations face more serious security threats than other technology consumers. In matters ranging from national defense to protection of citizens' personal data, national governments and international organizations must place security at the forefront of their information-technology requirements. One way Microsoft is working to address these security challenges is through the Government Security Program (GSP) -a global initiative that provides national governments and international organizations with access to Windows source code and other technical information they need to be confident in the security of the Microsoft Windows platform.

This document describes the processes and procedures for the GSP. The purpose of the guide is to provide program participants the information they need to understand the GSP program in more detail.

Table of Contents

Introduction

The Government Security Program (GSP) is one important facet of Microsoft's efforts to help address the unique security requirements of governments around the world. The GSP provides national governments access to Windows® source code and the information they need to be confident in the security of the Microsoft® Windows platform. This program embodies the principles of Microsoft's Trustworthy Computing and Shared Source initiatives, and is built upon the cornerstones of transparency and partnership.

Benefits

Participation in the GSP affords national governments the following benefits:

- SSL-secured online access to source code for current versions, beta releases and service packs of Windows 2000, Windows XP, Windows Server 2003 and Windows CE
- Engineering-level understanding of Windows architecture through expansive disclosure of Microsoft technical information
- The enhanced ability to conduct security audits and to design, build and maintain demonstrably secure computing environments
- Improved troubleshooting and systems-optimization capabilities
- Access to cryptographic code and development tools, subject to U.S. export regulations;
- Communication and collaboration with Microsoft security professionals
- Opportunities for visits by agency representatives to Microsoft development facilities in Redmond, Washington.

Participation in the Government Security Program begins by entering into a GSP Source Code Agreement. The GSP Agreement establishes a standard three-year

relationship, and sets forth all the basic elements of program participation. It describes the available types of license grants to access and use Microsoft source code, and establishes certain limitations to those grants. It specifies that source code access is via MSDN Code Center Premium for the Government Security Program using smartcards. It also provides for protection of Microsoft intellectual property, and invites feedback and communication. The GSP Agreement's terms apply both to employees and to approved agency contractors, and the document takes effect upon the signing of at least one project-oriented GSP Authorization.

After the legal documents are signed and necessary information obtained, the Microsoft GSP Team provides the participating government agency with the smart cards required to access Code Center Premium. The agency can then commence its security review. In the process of conducting its security review, the agency might have additional questions or needs for information or documentation that would help the agency better understand a particular aspect of the Windows. Once the agency identifies the additional information needed, the agency is invited to communicate such requests to Microsoft. In addition, the agency may elect to visit the Microsoft campus to review various aspects of Windows source-code development, testing and deployment processes, to discuss existing and potential projects with Microsoft security experts, and generally to interact with Microsoft staff.

Roles and Responsibilities

Agencies are governmental organizations that are authorized by Microsoft to access source code. To facilitate coordination of the government security review, where convenient for the participating government or international organization, the GSP Code Agreement envisions a single national government division or authority as the sponsoring agency within each participating nation. This agency executes the three-year GSP Code Agreement and may conduct the security review on behalf of the national government. The sponsoring or lead agency has direct access to MSDN Code Center Premium for the Government Security Program, and may authorize other government agencies for project-specific source-code access during the term of the GSP Agreement. Within such project-specific authorizations, Microsoft-approved contractors of sponsored agencies may be afforded code-access privileges identical to those of authorized agency employees.

A lead agency must sign a Source Code Agreement and a Source Code Authorization with Microsoft. A Source Code Agreement sets the overall framework for how the lead agency and their government will work with Microsoft on the GSP. A Source Code Authorization is the license grant of the source code for a specific security review project the agency is conducting.

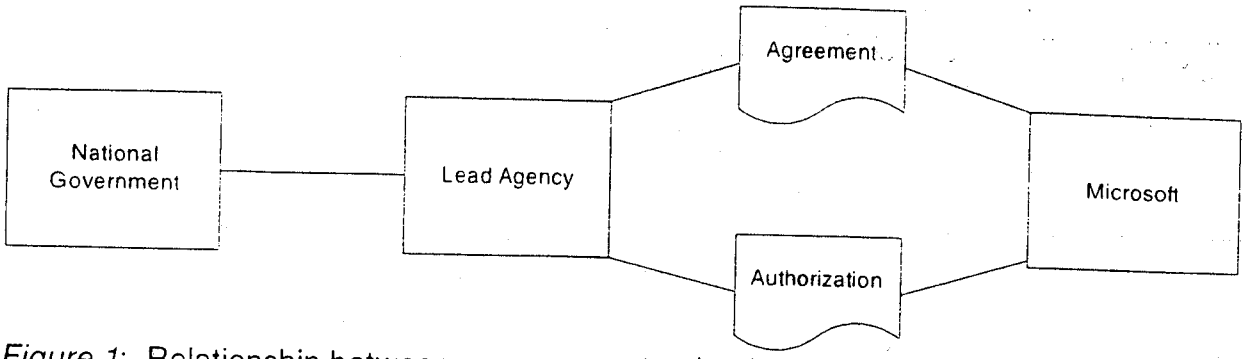


Figure 1: Relationship between a government, a lead agency and Microsoft

A lead agency may authorize other government agencies (sponsored agencies) to access Microsoft source code for a specific security review project. A sponsored agency must sign an authorization with a lead agency and Microsoft in order to obtain access to the source code. A lead agency may authorize multiple sponsored agencies for multiple security review projects.

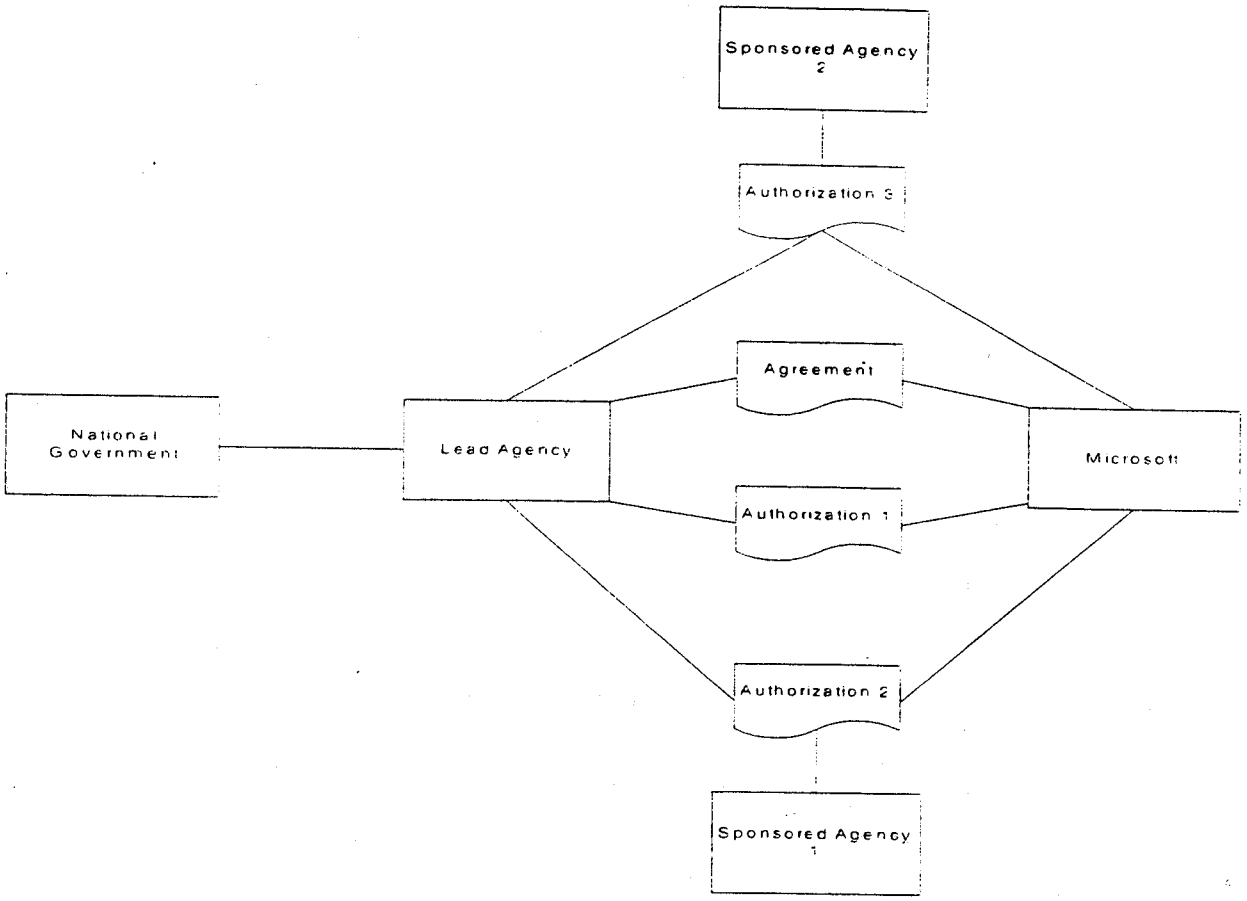


Figure 2: Relationship between a government, a lead agency, multiple Sponsored Agencies and Microsoft

Once a sponsored agency is authorized by the lead agency and Microsoft to access the source code on behalf of the national government, the sponsored agency has a direct relationship with Microsoft.

There are two types of personnel involved in the GSP program, agency employees and contractor/consultants. Agency (lead or sponsored) employees are people who are employed full time by the organization. Contractor/consultants are individuals who are not full time employees of the agency, but are doing work for hire for the organization. An employee must be listed by the government in the Code Center Premium smart card fulfillment form. A contract/consultant must sign an Additional Personnel Exhibit with the agency and Microsoft in order to access the source code.

Note: If a sponsored agency would like to hire a contract/consultant for assistance with a security review covered under their authorization, the lead agency does not need to sign the Additional Personnel Exhibit. The Additional Personnel Exhibit is signed only by MS and the sponsored agency.

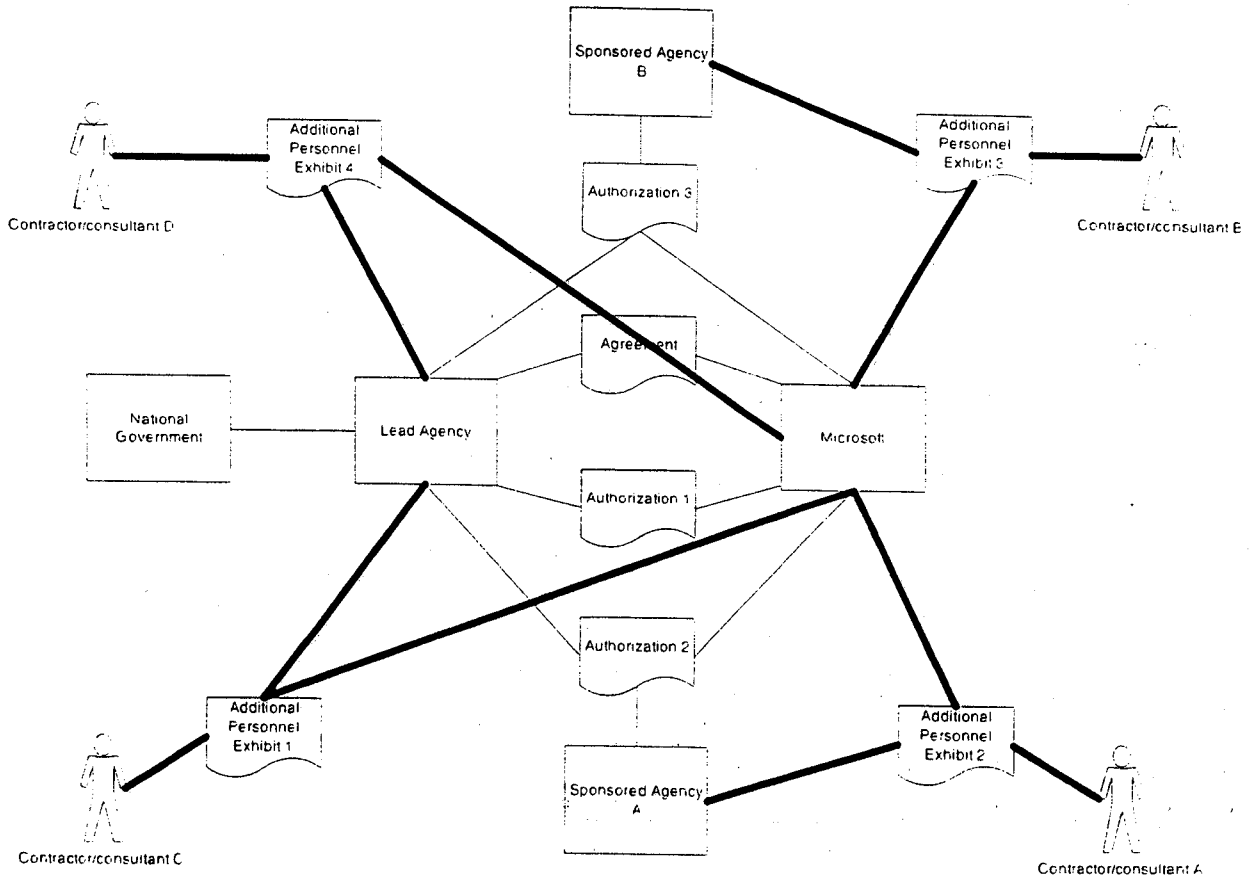


Figure 3: Relationship between contractor/consultants, agencies and Microsoft. Heavy lines denote the relationship between the signatories on the Additional Personnel Exhibits.

GSP lifecycle

The following sections of this document will detail the GSP program lifecycle. The phases of the GSP lifecycle are:

1. Sign Agreement and Authorization
2. Obtain access to the GSP Code Center Premium (CCP) website
3. Review Code
4. Attend Source Code Workshop
5. Visit Redmond
6. Request additional information
7. Continue with review process
8. Leaving GSP

1 – Sign Agreement and Authorization

Lead Agency

There are two major steps for a lead agency to sign up for the GSP, signing the GSP Source Code Agreement and signing the GSP Authorization. The Source Code Agreement is a three year contract that defines the framework for the licensing source code from Microsoft. The GSP Authorization is an annual project-specific source-code access license. The standard authorization contains a reference grant. Additional Authorizations may be entered into if additional projects are jointly identified and agreed.

The parties involved in the discussion and execution of the agreement and authorization are the lead agency and Microsoft.

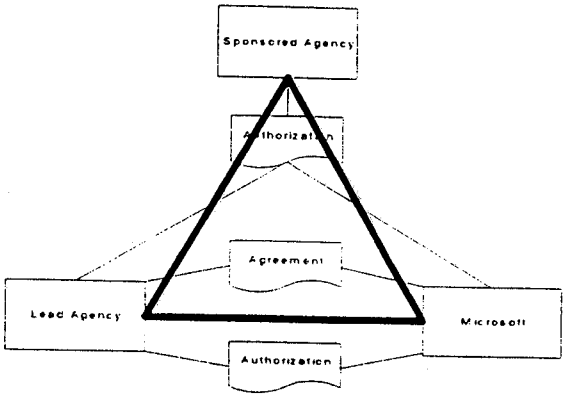
Sponsored Agency

In order for a sponsored agency to sign up for the GSP, the sponsored agency must be nominated by a lead agency and then sponsored agency must sign an Authorization with Microsoft and the lead agency.

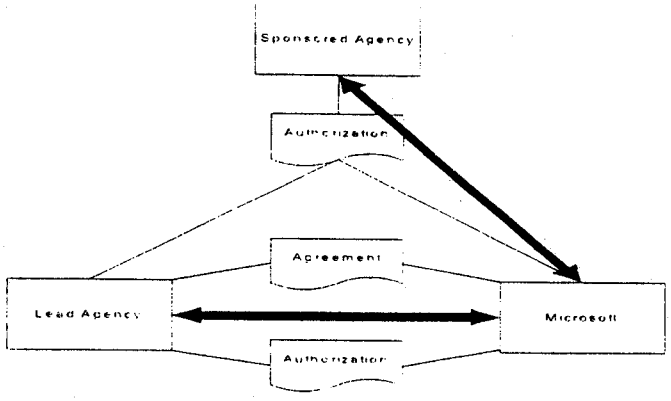
The sponsored agency, lead agency and Microsoft work together to identify and agree to the scope of the authorization for a sponsored agency. After the authorization is signed, the sponsored agency works directly with Microsoft.

NOTE: After the sponsored agency's Authorization is signed, the lead agency is not required to be involved with the sponsored agency's relationship with Microsoft unless the Authorization scope changes or unless specifically requested by the Lead Agency.

Phase 1: While the scope of the authorization is being identified and agreed, the lead agency, sponsored agency and Microsoft are all in communication about the project specific work of the sponsored agency. The heavy lines in the diagram below denote the communication channels, while the thin lines denote the contractual relationships.



Phase 2: After the Authorization is signed, the lead agency and the sponsored agency may have separate communication processes with Microsoft, unless the Lead Agency requests that it be kept included in all communications between the Sponsored Agency and Microsoft. The heavy lines in the diagram below denote the communication channels, while the thin lines denote the contractual relationships.



2 - Obtain access to GSP CCP website

Once the lead agency Source Code Agreement and the agency (lead or sponsored) Agreement has been fully executed, Microsoft will send the agency contact a welcome letter and account request form.

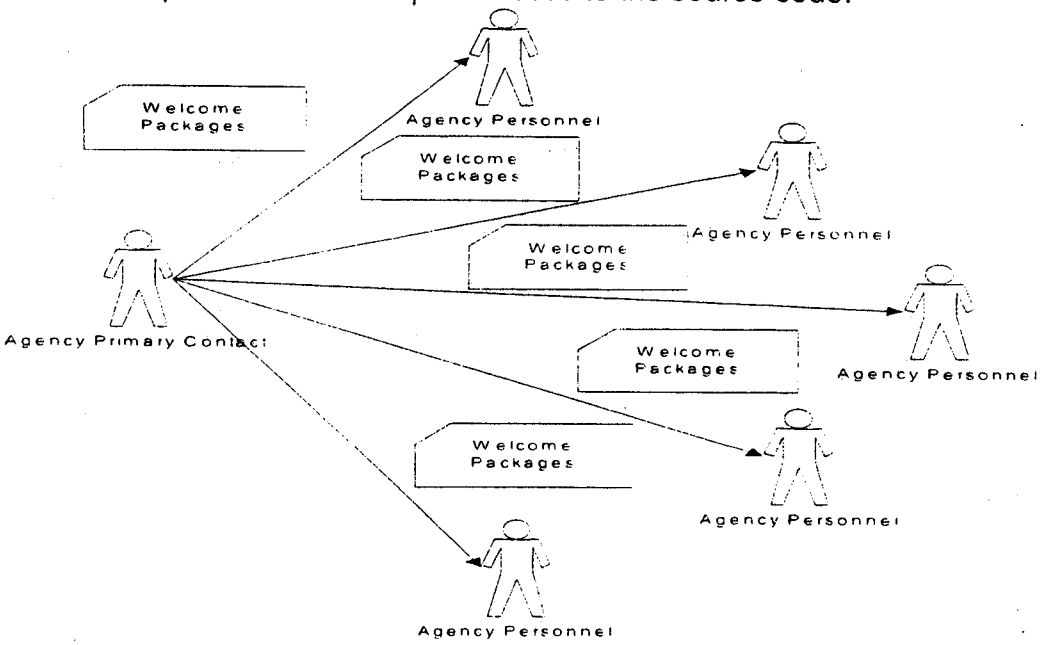
Note: In the case of a sponsored agency, at this point, the sponsored agency can communicate directly with Microsoft, without lead agency involvement. Absent a request by the Lead Agency for a different process, the lead agency is not required to be involved unless or until an Authorization is re-scoped.

The agency primary contact will fill out the account request form for each person who requires access to the source code, and send the completed form back to Microsoft. This includes employees as well as contractor/consultants with fully executed Additional Personnel Exhibits.

Once the account request form is received by Microsoft, Microsoft sends the first of two packages, Welcome Package 1, to the primary contact for the agency. This package includes the smart cards required to access the Code Center Premium website.

After Welcome Package 1 is sent, Welcome Package 2 is sent to the agency's primary contact. Welcome Package 2 includes the smart card reader and the smart card reader software installation CD.

The agency primary contact is responsible for distributing the smart cards, smart card readers and the software installation CDs to the personnel listed in the account request form that require access to the source code.



Once all GSP Welcome Kit components are received by the agency personnel, the agency has two choices. Either the primary contact sends an email to Microsoft requesting PINs for all new users, or each new user sends an individual email to Microsoft to request a PIN. Microsoft will send the PINs to the individuals directly or to the primary contact, depending on the agency's preference.

At this point, the new user may access Code Center Premium for GSP.

3 - Review Code

Once an agency is authorized to view the source code and they have confirmed access via the MSDN Code Center Premium site, they can start conducting their security review, pursuant to their specific authorization. During the review, the participants may view and search the code. The review should physically take place in authorized government facilities specified in the GSP Authorization. The participants are not authorized to view the code from home or any other unauthorized locations.

Any issues, questions or feedback for the Code Center Premium website should be sent to Microsoft at cpfeed@microsoft.com. All other issues, questions or feedback relating to participation in the Government Security Program should be sent to gspteam@microsoft.com

Sharing information about the review within the Government

Only personnel authorized by the agency may view the Microsoft source code as set forth in the GSP Agreement and Authorization. The authorized personnel may approve use of a product or application based on their knowledge of the source code, but may not share any details of the approval or review process that would list or imply the contents of the source code. For instance, authorized personnel may share with the rest of the agency or other governmental agencies within your country that Windows XP professional is approved by their group as a secure desktop application. Authorized personnel may not share that they came to this conclusion because the architecture is designed in a specific way, or that files X, Y and Z are approved because they do not contain specific vulnerabilities.

Reporting Security Vulnerabilities During Review

MSRC processes for investigating security vulnerabilities

The goal of the Microsoft Security Response Center is to perform a thorough investigation of every security vulnerability reported. The process for vulnerability resolution is described in this section.

1. **Vulnerability reported by agency personnel**
Report potential security vulnerabilities to gspsec@microsoft.com with the following information listed below. Information underlined is required, while all information is recommended in order to provide the best service to our GSP participants. Bugs or vulnerabilities that did not arise as a result of the review of the source code and that are not related to your agency's participation in the GSP should be sent to: security@microsoft.com.

- **Contact Information**

May we contact you about this report?

- **Computer information**

Manufacturer and model of your computer:

Have you installed any additional hardware on the system?

What operating system are you using?

Have you installed any operating system service packs?

- **Context for Report**

Did this report arise out of usage or access to source code or out of other usage of Microsoft products?

- **Affected Product**

What product are you reporting the security vulnerability in?

- **Vulnerability Information**

Please describe the flaw in the product:

Is the flaw present in the product in the default configuration?

Please tell us how to duplicate the problem in our laboratory (step-by-step instructions or a program that demonstrates the flaw):

Please describe how someone might mount an attack via the flaw:

Please describe what the result of a successful attack would be:

Please provide any additional information that might be helpful in investigating this issue:

Why we need this information
First and foremost, we require the requested information to ensure that as GSP participants, your feedback is acknowledged and acted upon as quickly as possible. The following section explains why Microsoft is asking for such detailed vulnerability information.

- **Contact Information**

We ask for contact information because we frequently need to ask follow-up questions of the person who submitted a report. For instance, we may discover in the course of investigating a report that we need some additional information about the problem. If we can't contact the person who submitted the report, we may be unable to complete the investigation. Likewise, we like to provide periodic status updates to the person who submitted the report, but we can only do this if we have contact information.

You can provide as much or as little contact information as you'd like. We will not share this information outside of Microsoft, nor will we add you to any mailing lists or customer databases.

- **Information about Your Computer**

Before we can correct a product flaw, we have to see it for ourselves and understand when and why it happens. We start every investigation by setting up a computer in our laboratory that's a duplicate of the one used by the person filing the report. Once we've seen the problem there, we can determine whether it affects a narrow range of systems or is a general problem.
We do not require any identifying information about your system. For instance, we do not need (and do not ask for) information like your computer's serial number or the Product ID for your operating system.

- **Context of Report:**

We need to understand in what context the bug or vulnerability was identified. Particularly, we would like to know if your review of the source code led you to identify a bug that would otherwise have not been identified. If the report does not relate at all to participation in the GSP, we need to refer you to security@microsoft.com.

- **Affected Product**

In order to investigate a vulnerability report, we need to know what product is involved, with as much detail as possible about the version, service pack, and

previously applied service packs. However, we do not require any identifying information such as Product IDs.

- **Vulnerability Information**

We ask for quite a bit of information about the vulnerability, but all of it is necessary in order for us to fully understand the issue. Here's what we need to know, and why we need it:

What the product flaw is. Before we can evaluate whether there's a security vulnerability, we first need to know what's wrong with the product's operation. By analogy to home security, we need to know what's wrong with the front-door lock before considering what a burglar could do once he's inside the house.

Step-by-step instructions for duplicating the flaw. We want to ensure that we've done the most thorough investigation possible. To do this, we need to be able to see exactly what you've seen on your own system. The more precise information you can provide for duplicating the problem, the more effective an investigation we'll be able to do.

Attack scenario: A security vulnerability comprises both a flaw and a way to exploit it. Our security teams are up to date on the latest attacks, and are very creative about devising new ones, but we'd still like to hear your thoughts about how a flaw might be exploited. You may have developed an entirely new scenario that has never occurred to us.

Attack outcome. Equally important as how someone might exploit a vulnerability is what they might gain by doing so. Understanding what an attacker could do through a security vulnerability lets us accurately assess the seriousness of the issue.

Many people choose to provide the information in the form of a program that demonstrates the problem. This is not a requirement -- it's usually sufficient to provide us with detailed information. If you do decide to provide a demonstration program, we recommend that you ensure it can't be used to cause harm to other users' systems. Similarly, we strongly recommend against testing a vulnerability on other users' systems. as this is illegal in most countries.

2. **MS Security Response team reviews and prioritizes issues reported.**
3. **MS reproduces the vulnerability.**
4. **If deemed necessary, MS develops and tests fix and accompanying documentation.**
5. **Fix is distributed back to customers and lessons learned are incorporated in development practices.**

4 - Attend Source Code Workshop

Upon request and if needed, Microsoft can arrange for source code workshop on location or at Microsoft campus (costs associated). The workshop is conducted by Azius, an independent vendor contracted by Microsoft to provide training around the Windows source code

5 - Visit Redmond

As part of the program, representatives of participating government agencies may opt to visit Microsoft development facilities to review various aspects of Windows source-code development, testing and deployment processes, to discuss existing and potential projects with Microsoft security experts, and generally to interact with Microsoft staff. For the government participants, this represents an occasion for gaining valuable insights into Windows security. For Microsoft, the visit offers an invaluable opportunity to receive feedback from agency representatives. Visiting agencies will be asked to outline specific projects and objectives prior to arrival, so that Microsoft can best develop a customized, rewarding itinerary.

The objectives of an agency visit to Redmond are: to review source code that may not be available via CCP, allow the participants to see how Windows is built, exchange information and ideas with Microsoft development teams directly, and further project specific work requested by participants.

The process for coordinating an agency visit to Redmond is as follows:

1. GSP Agreement and Authorization Signed
2. Agency provided information must be received at least four weeks prior to proposed visit
    a. Curriculum Vitae of agency visitors
    b. Statement of primary objective of agency visit - what they want to learn from or communicate to Microsoft

c. Agency's agenda including at least three specific things they want to achieve during their visit

3. Welcome Packet sent to participants, which includes:
   a. Information on how to arrange travel, places to stay
   b. Map and driving directions from airport
   c. 1st day contact information
   d. Profile of the program
   e. Copy of agenda (subject to change)
   f. Forms to fill out (i.e. NDA)
   g. Listing of local attractions
   h. Best places to go guide

6 - Request Additional information

As a part of the program, Microsoft provides documentation to help GSP participants get more benefit and better understanding of security. As the agency conducts their security review, they are encouraged to send the Microsoft GSP team feedback on the product under review and any questions or requests for additional information or documentation that may arise as a result of the review. The GSP participants may send these requests and questions to Microsoft using the alias gspteam@microsoft.com.

Authorization Renewals

Authorizations are valid for one year from the date signed. If after one year, the authorization scope does not need to be amended (for a lead or sponsored agency), the authorization is automatically renewed, subject to the terms and conditions of the applicable authorization. If, subject to the mutual agreement of the parties, the scope of the authorization for a lead agency does change, the lead agency and Microsoft may negotiate a new Authorization. If, subject to the mutual agreement of the parties, the scope of authorization for a sponsored agency does change, the sponsored agency and the lead agency may work with Microsoft to negotiate a new Authorization.

7 - Continue with review

The agency will continue with review process based on greater understanding from visit and documentation. During the ongoing review, the agency is encouraged to send feedback to Microsoft about security vulnerabilities found, request information as needed and identify any future projects to conduct with Microsoft.

8 - Leaving the GSP program

When the license to any source code ends, the agency must return or destroy all copies of source code and any associated materials in the agency's possession and, upon request from Microsoft, provide Microsoft with a letter stating that all copies of the Source Code have been returned or destroyed.

Microsoft®

Government Security Program: Fact Sheet

Overview The Government Security Program (GSP) is one important facet of Microsoft's efforts to help address the unique security requirements of governments around the world. The GSP provides national governments access to Windows® source code and information they need to be confident in the security of the Microsoft® Windows platform. This program embodies the principles of Microsoft's Trustworthy Computing and Shared Source initiatives, and is built upon the cornerstones of transparency and partnership.

Benefits Participation in the GSP affords national governments the following benefits:

- Online access to source code for the most current versions, beta releases and service packs of Windows 2000, Windows XP, Windows .NET Server 2003 and Windows CE;
- Engineering-level understanding of Windows architecture through expansive disclosure of Microsoft technical information;
- Enhanced ability to conduct security and privacy audits and to design, build and maintain demonstrably secure computing environments;
- Improved troubleshooting and systems-optimization capabilities;
- Access to cryptographic code and development tools, subject to U.S. export regulations;
- Communication and collaboration with Microsoft security professionals; and
- Opportunities for visits by agency representatives to Microsoft development facilities in Redmond, Washington.

Program Details The program provides zero-cost "smart-card" access to source code via MSDN® Code Center Premium for the Government Security Program, an online resource that enables authorized government personnel to browse, search and download source-code files from approved locations.

- *GSP Source Code License Agreement*: The GSP Agreement sets forth all basic elements of the program, and specifies the parties' respective rights and obligations. Its terms are straightforward and applied consistently among participating nations. It is valid for a period of three years.
- *Sponsoring Agency and Authorized Agencies*: Typically, one national government authority or department in each participating nation serves as the sponsoring agency. This agency signs the GSP Agreement, typically conducts the security review on behalf of the national government and has direct access to MSDN Code Center Premium for the Government Security Program. The sponsoring agency may authorize other government agencies for annual, project-oriented source access during the term of the GSP Agreement.
- *GSP Authorizations*: The GSP Authorization establishes the license grant and sets forth more specific terms defining each security project launched under the GSP by the sponsoring agency or any authorized agency. It is executed by the agency undertaking the project. The term of the authorization is one year, and is renewable. Each GSP Authorization becomes part of the GSP Agreement.
- *Visit to Microsoft Facilities*: Representatives of licensee agencies may opt to visit Microsoft development facilities in Redmond to discuss critical projects with Microsoft security experts and to review the Windows source-development process. Visiting agencies are asked to outline specific projects and objectives prior to arrival, so that their representatives' itineraries may be optimized.

Questions Additional questions regarding the Government Security Program should be directed to the Microsoft GSP Team at GSPTeam@microsoft.com.

U.S. GOVERNMENT SECURITY PROGRAM SOURCE CODE AGREEMENT

This U.S. Government Security Program Source Code Agreement ("GSP Code Agreement") is an agreement between Microsoft Corporation ("Microsoft") and the National Institute of Standards and Technology ("NIST"). It becomes effective on _____ ("Effective Date").

INTRODUCTION

This GSP Code Agreement is a framework for licensing source code from Microsoft, including information NIST obtains from or about the source code (collectively called "Source Code"). This GSP Code Agreement describes terms that always apply, and must be accompanied by one or more attachments with specific information ("Authorizations") that describe the Source Code to be provided, what can be done with it, and for how long. The GSP Code Agreement and any Authorizations together become the full Agreement ("Agreement"). The license to access Source Code begins when NIST and Microsoft sign both this GSP Code Agreement and any associated Authorizations.

1. AUTHORIZED PERSONNEL AND PROTECTING OF SOURCE CODE

1.1 NIST will act as a central coordinating agency for Source Code under this Agreement. NIST may, with Microsoft's prior written approval, designate additional agencies in the U.S. Government to access Source Code ("Sponsored Agencies"), as described in an Authorization.

1.2 The Agreement applies to all individuals that access the Source Code ("Personnel").

1.3 NIST will sign one GSP Code Agreement and the initial GSP Authorization. NIST may in the future sign additional Authorizations to support other efforts involving Source Code as NIST, any Sponsored Agencies, and Microsoft may mutually agree.

1.4 NIST and Microsoft agree that this GSP Code Agreement will not be made public unless NIST is required by law to do so or NIST and Microsoft otherwise mutually agree. NIST agrees to immediately notify Microsoft in the event a third party requests access to the GSP Code Agreement or other related documentation. Such notification will be made prior to any information release so that Microsoft can take appropriate legal action to protect its interests.

1.5 Contractors or consultants supporting NIST or Sponsored Agencies will have the same rights and obligations NIST has under the Agreement (and references to "Personnel" in the Agreement include such contractors and consultants as applicable), only if such contractors and consultants (a) are legally obligated by the U.S. Government to abide by the same terms that apply to other Personnel under the Agreement and (b) have been approved in writing by Microsoft on a separate Additional Personnel exhibit.

1.6 The Source Code is a highly valuable trade secret of Microsoft and confidential information. When Microsoft makes the Source Code available under the Agreement, NIST agrees to protect such information in accordance with the requirements of the Trade Secrets Act, 18 U.S.C. 1905. In addition, Microsoft asserts that the terms of this Agreement are exempt from disclosure under Section (b)(4) of the Freedom of Information Act because they constitute trade secrets and privileged and confidential commercial information obtained from Microsoft.

NIST

1.7 If NIST or any Sponsored Agency are required by a court or any other authority to disclose any portion of the Source Code, NIST must give Microsoft immediate notice of the order so that Microsoft can seek an appropriate protective order (or equivalent).

1.8 [(b)(4)]

- Contractors and consultants can be used to fill any Personnel slot in the access system, provided they have been properly qualified as described above in Section 1.5.
- Personnel will access the Source Code only in the same manner and location as they would access NIST's most sensitive similar confidential information, as described in the Authorization Form, and will not permit any other person to view or access the Source Code in any way.

2. ENABLED LICENSE GRANTS. This Section describes the rights ("License Grants") NIST or any Sponsored Agency may obtain for Source Code. An Authorization, once signed by NIST, the Sponsored Agency and Microsoft, specifies the License Grant that applies to Source Code specified in the Authorization, and may include additional rights and obligations as NIST, the Sponsored Agency and Microsoft may mutually agree.

2.1 Reference. A "Reference Grant" permits NIST or the Sponsored Agency to use Source Code as a reference, in "read only" form, for the purpose specified in the Authorization. NIST or the Sponsored Agency may use the Source Code in digital or printed form as supplied by Microsoft. NIST or the Sponsored Agency may also view it using a debugger.

2.2 [(b)(4)]

2.3 Recommended Services. If Microsoft technical personnel assessing a proposed or current Authorization determine that for the success of the work described in an Authorization it is necessary to retain the services of Microsoft Consulting Services, Microsoft Product Support Services or a qualified third party service provider ("Recommended Services"), NIST or a Sponsored Agency may enter into an agreement for such services in accordance with standard terms and conditions for such services. In the event NIST or the Sponsored Agency does not obtain the Recommended Services, NIST or the Sponsored Agency acknowledges that the success of the associated work may be negatively impacted.

2.4 Condition to License Grants. As a condition of each license grant, NIST or a Sponsored Agency will not take any action that would (a) create, or purport to create, obligations for Microsoft with

respect to the Source Code or any derivative work thereof; or (b) grant, or purport to grant, to any third party any rights or immunities under Microsoft's intellectual property or proprietary rights in the Source Code or any derivative work thereof.

2.5 No Other Licenses. The parties agree that use of certain interfaces or data structures within the Source Code is unsupported, and may create additional support burdens for the U.S. Government and Microsoft or adversely affect the user experience with Microsoft's products, or other products created for a Microsoft platform. Accordingly, Microsoft grants no right under the Agreement to use the Source Code for the purpose of discovering and/or using interfaces (e.g. functions, protocols, on-disk or in-memory storage structures) other than those published by Microsoft and made publicly available (e.g., via Software Development Kits, Driver Development Kits, Microsoft Developer Network). All rights not expressly granted are reserved by Microsoft.

2.6 Comments and Suggestions. Microsoft invites NIST's or a Sponsored Agency's comments and suggestions on the Source Code and other product-related technical and operational information that Microsoft may disclose to NIST or a Sponsored Agency. If NIST or a Sponsored Agency gives Microsoft comments and suggestions regarding bug fixes, enhancements or other modifications to the Source Code or other such information, Microsoft may, in connection with Microsoft products and services use, disclose or otherwise commercialize in any manner, those comments and suggestions in any way it wants, entirely without any obligation or restriction based on intellectual property rights or otherwise.

2.7 Source Code and Software Development Kit Improvements. NIST agrees to use best efforts (a) to promptly notify Microsoft of any security concerns NIST may have as a result of NIST's or a Sponsored Agency's use of the Source Code, and (b) to provide Microsoft with comments and suggestions that might improve the effectiveness of any Software Development Kits that support efforts being performed by NIST or a Sponsored Agency for which Source Code is being used.

3. NO WARRANTY. MICROSOFT PROVIDES SOURCE CODE TO NIST AND SPONOSRED AGENCIES WITHOUT ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY, NOT EVEN THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR THE WARRANTY OF TITLE OR NON-INFRINGEMENT.

4. LIMITATION OF LIABILITY. NIST AGREES THAT MICROSOFT WILL NOT BE LIABLE UNDER THE AGREEMENT FOR ANY INDIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL OR PUNITIVE DAMAGES.

5. TERM & TERMINATION

5.1 Term. This GSP Code Agreement is in effect for 3 years from the Effective Date. The term of a license grant for Source Code is specified in each Authorization. The term of an Authorization may be shorter than this GSP Code Agreement but can never be longer. In addition, this GSP Code Agreement and any Authorizations may end earlier as described below.

5.2 Ending. In the event any unauthorized disclosure of the Source Code is discovered, or if Microsoft reasonably determines that there has been a breach of the Agreement, Microsoft may immediately terminate this GSP Code Agreement or any Authorization in its sole discretion. Either party may end this GSP Code Agreement or any Authorization by giving the other party 90 days' written notice. If this GSP Code Agreement is ended, all Authorizations end. If only a

particular Authorization is ended, this GSP Code Agreement and other Authorizations, if any, are not affected.

5.3 Surviving Terms. Even if this GSP Code Agreement ends, the following terms remain in effect: Sections 1, 2.4, 2.5, 2.6, 3, 4, 5, 7, 8 and 9. In addition, in the event NIST or a Sponsored Agency grants Microsoft any licenses under this Agreement, such licenses will survive even if this Agreement ends.

5.4 Returning Items. When NIST's or a Sponsored Agency's license to any Source Code ends, NIST or the Sponsored Agency must immediately return to Microsoft or destroy all copies of that Source Code and any associated materials such as smart cards. If Microsoft requests, NIST agrees that a properly authorized official of NIST or the Sponsored Agency will provide Microsoft with a letter stating that all copies of the Source Code have been returned or destroyed.

6. NOTICES

6.1 If NIST or Microsoft need to send a notice under the Agreement, the notice will be considered given one day after delivery to a commercial courier service using tracking capabilities and overnight or similarly expedited delivery, postage prepaid. All notices must be addressed as follows:

To NIST:		To Microsoft:	
_____		Microsoft Corporation	
_____		One Microsoft Way	
_____		Redmond, WA 98052-6399 USA	
Attention:	_____	Attention:	Platforms Business Management
Phone:	_____	Phone:	+001 (425) 882-8080
Fax:	_____	Fax:	+001 (425) 706-7329
Email:	_____	Email:	gspteam@microsoft.com
		Copy to:	Law & Corporate Affairs
		Fax:	+001 (425) 706-7409

6.2 Either NIST or Microsoft may change these addresses by giving notice of the change.

7. GOVERNING LAW/VENUE/ATTORNEY FEES. The Agreement will be governed by the laws of the United States of America. NIST agrees that the United Nations Convention on Contracts for the International Sales of Goods will not apply to the Source Code under the Agreement.

8. LIABILITY. NIST will be fully responsible for the full compliance by the U.S. Government's personnel, contractors and consultants with all obligations under the Agreement.

9. OUTCOME IF SOME SECTIONS ARE INVALID. If a part of the Agreement, other than Sections 1, 2.4, 2.6, 3, 4, 10 or 11, is held by a competent court to be unenforceable, the rest will remain in effect. If Sections 1, 2.4, 2.6, 3, 4, 10 or 11 are held by a competent court to be unenforceable, the Agreement ends immediately.

10. NIST CANNOT ASSIGN THE AGREEMENT. If NIST attempts to assign the Agreement for any reason, the Agreement ends immediately. As used in the Agreement, the term "assign" includes any attempt to shift responsibility for or control of any performance under the Agreement to other than NIST or a Sponsored Agency.

11. APPROVALS AND ELIGIBLE SOLICITATIONS.

11.1 NIST or a Sponsored Agency must, at NIST's or a Sponsored Agency's expense, obtain and maintain any approvals, consents, licenses, authorizations, declarations, filings, and registrations as may be necessary or advisable for NIST's or the Sponsored Agency's performance under the Agreement. NIST or a Sponsored Agency must also pay (and reimburse Microsoft if Microsoft gets charged) for any sales taxes, use taxes and any other taxes imposed by any jurisdiction as a result of the entry into this Agreement, the performance of any of its provisions, or the transfer of any property or rights under it.

11.2 The Source Code and any associated documentation is provided only with the rights and restrictions described elsewhere herein, and is not and will not be provided with "Restricted Rights" as provide for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227-7013 (OCT 1988).

12. EXPORT RESTRICTIONS. The Source Code is subject to U.S. export jurisdiction. NIST must comply with all applicable international and national laws that apply to it, including the United States Export Administration Regulations, as well as end-user, end-use and country destination restrictions issued by the United States and other governments. For information on exporting Microsoft products, see http://www.microsoft.com/exporting/.

13. CONTROLLING LANGUAGE. Although a translation may be provided for NIST's convenience, the Agreement has been executed in the English language, which shall be the sole and controlling language used in interpreting or construing its meaning.

14. GRATUITOUS SOURCE CODE. If the Source Code is provided at no charge to NIST or a Sponsored Agency, it is the intent of Microsoft that the terms of this letter and the attached License Agreement/Product Use Rights be in compliance with all applicable federal law and regulations. All products are provided under this letter for the sole use and benefit of NIST or the Sponsored Agency for Agency purposes only, and are not provided for use by or personal benefit of any specific Agency employee

14. ENTIRE AGREEMENT. The Agreement, which includes any executed Authorizations, is the only agreement between NIST and Microsoft covering the subject matter of the Agreement. It supersedes all other contemporaneous agreements and communications on the subject. However, if there is a conflict between this GSP Code Agreement and an Authorization, the terms of the Authorization will prevail with regard to the subject matter in the applicable Authorization. The Agreement will not be modified unless NIST and Microsoft sign an amendment after the Effective Date. Neither NIST nor Microsoft waives the right to claim breach of contract unless the waiver is in a signed, written document. A waiver only applies to things described in that document; it does not apply to other breaches of contract.

We agree to everything in this GSP Code Agreement.

MICROSOFT CORPORATION	NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGYNIST
By	By
Name (print)	Name (print)
Title	Title
Date	Date