



BJA
Bureau of Justice Assistance
U.S. Department of Justice

Global Reference Architecture

Supervision Conditions Summary (SCS) Service Service Description Document

Version 1.0

April 2012



Global
Information
Sharing Standard

Global Standards

Global's collection of normative standards has been versioned independently and assembled into a package of composable, interoperable solutions specifically supporting an information exchange. The package is known as the Global Standards Package (GSP). GSP solutions are generally technically focused but also may include associated guidelines and operating documents. GSP deliverables include artifacts associated with many of the Global product areas, including but not limited to:

- **Global Reference Architecture (GRA):** Offers guidance on the design, specification, and implementation of services (and related infrastructure) as part of a justice Service-Oriented Architecture (SOA).
- **Global Service Specification Packages (SSPs):** Reference services that serve as the means by which the information needs of a consumer are connected with the information capabilities of an information provider.
- **Global Federated Identity and Privilege Management (GFIPM):** Guidelines and standards for establishing, implementing, and governing federated identity management approaches.
- **Global Privacy Technology Framework:** A framework for automating access control (in particular, privacy) policy as part of information exchange.

For More Information

For more information on the GSP and the Global Standards Council (GSC)—the Global group responsible for developing, maintaining, and sustaining the same—please visit <http://www.it.ojp.gov/gsc>.

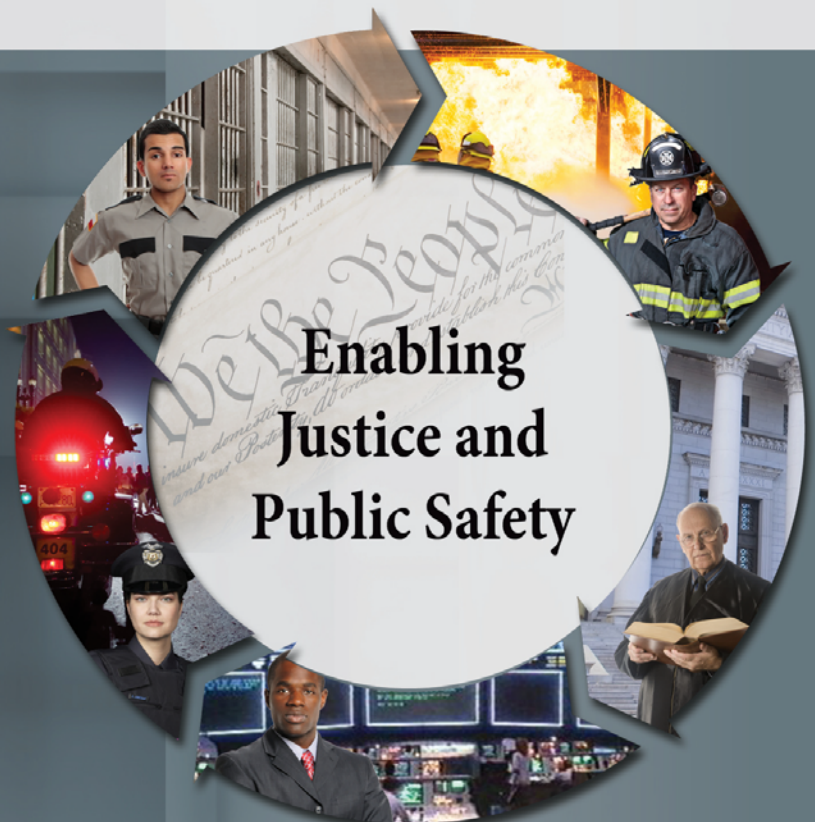


Table of Contents

1.	Document Introduction	1
2.	Service Overview	2
2.1	Purpose	2
2.2	Scope	2
2.3	Capabilities	3
2.4	Real-World Effects	3
2.4.1	Law Enforcement	3
2.4.2	Probation and Parole	3
2.4.3	Courts	3
2.4.4	Human Services	4
2.5	Summary	4
2.6	Description	4
2.7	Security Classification	4
2.8	Service Specification Package Version	4
3.	Business Scenarios	4
3.1	Primary Flow	4
4.	Service Interoperability Requirements	6
4.1	Service Assumptions	6
4.2	Service Dependencies	6
4.3	Execution Context	6
4.4	Policies and Contracts	6
4.5	Security	7
4.6	Privacy	7
5.	Service Model	7
5.1	Information Model	7
5.2	IEPD Reference	7
5.2.1	Data Inputs	8
5.2.1.1	Query Message	8
5.2.1.2	Response Message	8
5.2.3	Data Outputs	8
5.2.4	Data Provenance	8
5.3	Behavior Model	8

5.3.1 Action Model	8
5.3.2 Process Model	9
Appendix A—References	12
Appendix B—Glossary	13
Appendix C—Document History	14

1. Document Introduction

In the context of the GRA and Service-Oriented Architecture [SOA] in general, a service is the means by which one partner gains access to one or more capabilities offered by another partner. Capabilities generate real-world effects that can be as simple as sharing information or can involve performing a function as part of a complex process or changing the state of other related processes. Government organizations have numerous capabilities and a multitude of partner organizations, both inside and outside of their traditional communities. There are significant benefits for these organizations to share information and have access to each other's capabilities. Achieving interoperability among these organizations requires alignment of business and technical requirements and capabilities. In addition, it is critical to have a consistent way of specifying these requirements and capabilities and sharing them across organizational boundaries. The GRA was developed to facilitate interoperability and to assist in meeting other key requirements common in a complex government information sharing environment. In order to achieve interoperability, a consistent approach must be defined to identify, describe, and package services and their interactions in many different technical environments, across multiple government lines of business, at all levels of government, and with partner organizations.

The GRA defines a service interface as “the means for interacting with a service.” It includes specific protocols, commands, and information exchange by which actions are initiated on the service. A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the “how” of the interaction. Since the service interface is the physical manifestation of the service, best practices call for service interfaces which can be described in an open-standard, machine-referenceable format (that is, a format which could be automatically processed by a computer).

A Service Specification is a formal document describing the capabilities made available through the service; the service model that defines the semantics of the service by representing its behavioral model, information model, and interactions; the policies that constrain the use of the service; and the service interfaces which provide a means to interacting with the service. A Service Specification is analogous to the software documentation of an Application Programming Interface [API]. It provides stakeholders with an understanding of the structure of the service and the rules applicable to its implementation. It gives service consumers the information necessary for consuming a particular service and service providers the information necessary for implementing the service in a consistent and interoperable way.

The main components of a Service Specification are the Service Description, one or more Service Interface Descriptions, and the schemas and the samples used to implement and test the service.

A Service Description contains information about all aspects of the service which are not directly tied to the physical implementation of the service; in other words, the service interface. A Service Interface Description is a description of the physical implementation; specifically, the service interface used in a specific implementation of the service.

This document is designed as a Service Description for the Supervision Conditions Summary (SCS) Service.

2. Service Overview

2.1 Purpose

The SCS Service provides a summary of supervision (e.g., probation and parole) conditions to which a specific person is subject to. This capability enables exchange partners to quickly and efficiently perform assessments, determine whether a subject is in violation of any supervision conditions, and support decision making throughout the criminal justice system.

2.2 Scope

The SCS Service provides a query/response mechanism for interested parties to obtain a summary of any supervision conditions that apply to a specific individual. The specification places no restrictions on the lines of business that might participate in such an exchange, although probation and parole agencies will typically act as responding entities.

The SCS Service assumes that the service consumer has the necessary information to uniquely identify the subject (person) of interest to provider systems. As such, identity resolution is not within the scope of the SCS Service. The SCS Service, however, may be orchestrated with other services to provide this capability; for example, the Fingerprint Service¹ could be used to obtain a biometric identifier which could then be used in an SCS query message to uniquely identify the subject of interest. It should also be noted that the SCS information model is flexible enough to allow for other types of identifiers depending on the implementation.

Additionally, the SCS Service assumes that the service consumer is aware of the existence and location of the service provider; that is, the consumer system has the information necessary to route and deliver an SCS Query Message to the provider system. The SCS Service, however, may be orchestrated with other services to provide this capability. For example, the Person Information Availability (PIA) Service² could be used to determine that supervision condition information is available for an individual and how to obtain the details of such conditions. Using the information from the PIA response message, a consumer could then generate and send a detailed information request to an SCS provider system.

¹ Fingerprint (FP) Service Specification, Working Draft v 1.0.0.

² Person Information Availability (PIA) Service, Working Draft v 1.0.0.

2.3 Capabilities

1. Query Supervision Conditions
2. Receive Supervision Conditions

2.4 Real-World Effects

At a high level, the SCS Service provides consumers with a summary of the supervision conditions in effect for a specific person. This capability provides myriad real-world effects to service consumers that can be used throughout a government enterprise.

Across all lines of business, the service is used to quickly determine what, if any, supervision conditions a specific person is subject to. This enables effective decision making regarding the handling of an individual, promotes public safety and staff safety, and reduces redundant data entry.

The following examples illustrate how various entities could benefit from this capability. It should be noted, however, that use of this service is not constrained to the following lines of business.

2.4.1 Law Enforcement

During an encounter with a person, law enforcement officers can quickly ascertain whether that person is subject to or in violation of any supervision conditions.

2.4.2 Probation and Parole

Probation and parole officers can quickly identify an individual's supervision conditions for the purpose of making effective decisions relating to a person's housing, treatment needs, or additional supervision restrictions.

2.4.3 Courts

During court appearances, courts can quickly identify any supervision conditions currently in effect for a person. This information can be used to determine if violations occurred and ensure any additional conditions imposed by the court are compatible with existing restrictions.

2.4.4 Human Services

When performing an assessment, human services agencies can quickly obtain a person's supervision conditions to support treatment and monitoring decisions.

2.5 Summary

Businesses will use this service to quickly determine what, if any, supervision conditions are in effect for a specific person. Where applicable, source systems, record identifiers, and other metadata are provided to enable further inquiry of underlying data sources.

2.6 Description

The SCS Service provides mechanisms to support the query and retrieval of supervision condition information relating to a specific individual. Upon receiving a request message from a consumer system, the provider system searches for supervision condition information about the identified individual then returns a response message identifying the specific conditions and restrictions that apply to that individual.

2.7 Security Classification

The highest level of security classification for the information exchanged by this service is Sensitive But Unclassified (SBU). As a result, the service can be assigned a security classification of SBU.

2.8 Service Specification Package Version

This service specification is built based on version 1.0.0 of the Service Specification Package.

3. Business Scenarios

Businesses will use this service to determine what, if any, supervision conditions are currently in effect for a specific individual.

3.1 Primary Flow

- A user or system seeks to determine what supervision conditions are in effect for a specific person.
- The Requesting System generates and submits a request message to the SCS Service. This message contains identifying information for the person of interest as well as other information to identify the requesting user and/or system.

- The SCS Service waits for an asynchronous response from the Responding System. Note that the Requesting System implementation must make provisions for handling timeouts and other exceptional conditions while waiting for this response.
- The Responding System searches for supervision conditions relating to the person of interest. The Responding System may choose to filter this information based on local policies or the identity of the requesting user or system.
- The Responding System generates and sends a response message to the Requesting System. The response message indicates what supervision conditions are applicable to the subject of interest or that no records could be found.

The following diagram depicts the primary process flow described above:

Supervision Conditions Summary

Supervision Conditions Request

Primary Process Flow

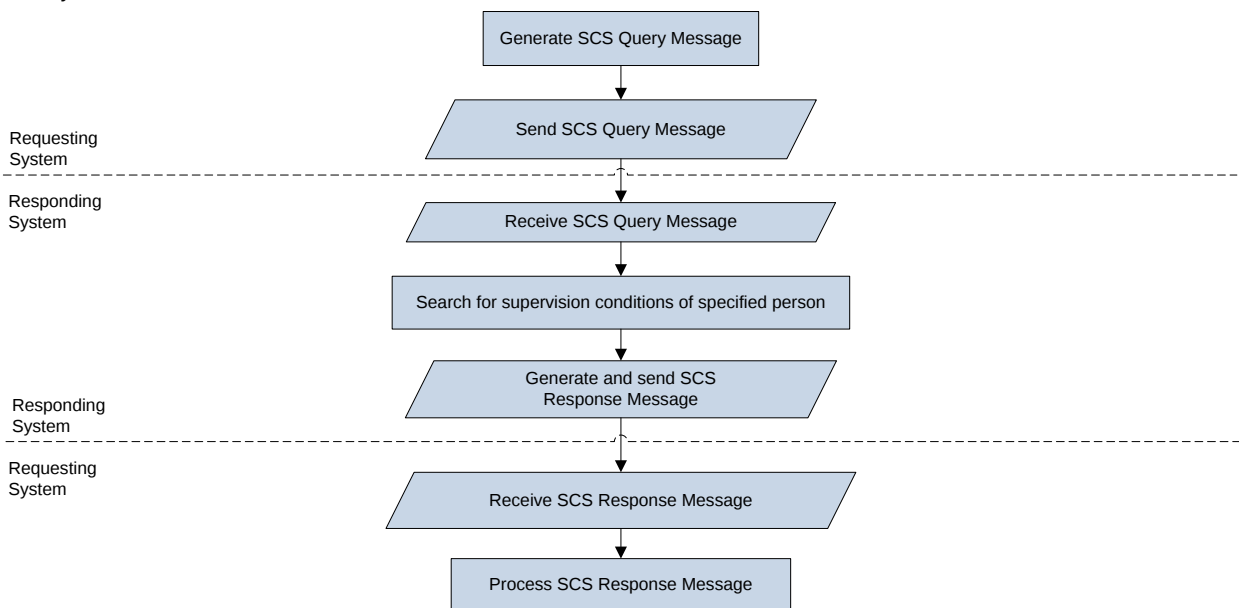


Figure 1: Primary Process Flow Diagram—Supervision Conditions Request

4. Service Interoperability Requirements

4.1 Service Assumptions

- All messages exchanged are stored in a log file for auditing purposes.
- All messages exchanged will require a synchronous acknowledgement of receipt.
- The acknowledgement of receipt will only contain metadata about the message. The metadata will consist of a timestamp and identifiers that uniquely identify the message.
- Messages other than the synchronous acknowledgement or fault (i.e., SCS Response message) are returned asynchronously. As such, Requesting Systems must implement a service endpoint to receive these responses.
- The service implementation has a means to identify and locate Responding Systems; that is, the service specification does not specify how the service might locate responding systems of interest. In practice, the identities of Responding Systems may be “hardcoded” in the service implementation, found using an electronic directory, or obtained through the use of another service such as PIA.

4.2 Service Dependencies

No dependencies have been identified at this time.

4.3 Execution Context

The service design will follow the GRA Execution Context Requirements.

4.4 Policies and Contracts

Participating entities will use Memoranda of Understanding (MOUs), Non-Disclosure Agreements (NDAs), Service-Level Agreements (SLAs), or other types of agency agreements, as appropriate, to document applicable policy requirements.³

³ See “Policy Documents” at <http://it.ojp.gov/default.aspx?area=nationalInitiatives&page=1015> for sample MOU (entitled GRA Information Sharing Enterprise Statement of Participation) as well as an SLA (Information Sharing Enterprise Service Level Agreement).

4.5 Security

- The service implementation must adhere to the rules of the Criminal Justice Information Services (CJIS) Security Policies.
- Due to the variety and complexity of the security rules associated with the messages exchanged by the SCS Service and the significant differences from jurisdiction to jurisdiction, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM is in place for the implementation of this service.

4.6 Privacy

- The MOUs between participating entities will further define specific privacy requirements.
- Due to the variety and complexity of the privacy rules associated with the messages exchanged by the SCS Service and the significant differences from jurisdiction to jurisdiction, it is recommended that a comprehensive authorization and access control mechanism based on GFIPM is in place for the implementation of this service. This would allow implementation of the guidelines defined by the Global Privacy Technical Framework.

5. Service Model

5.1 Information Model

The information exchanged by the service consists of a request message identifying the subject of interest and the requesting entity, a WS-RM-based acknowledgement or fault message, and a response message indicating the supervision conditions in effect for a person.

5.2 IEPD Reference

The SCS Service uses the American Probation and Parole Association (APPA) Supervision Conditions Information Exchange Package Documentation (IEPD) for all messages exchanged by the service. The IEPD is included in its entirety in the [artifacts/service model/information model](#) folder of the Service Specification Package.

5.2.1 Data Inputs

5.2.1.1 Query Message

An SCS *SupervisionConditionsQueryMessage* is used to submit a query request to the service. The message contains, at minimum, information to identify the subject of interest, information to identify the person and/or agency requesting the information, and metadata used to correlate a response with the request.

5.2.1.2 Response Message

An SCS *SupervisionConditionsResponseMessage* is used to asynchronously submit the results of the query to a requesting system. The message indicates what, if any, supervision conditions are in effect for the subject of interest and includes metadata indicating the owner of the data. Refer to the APPA Supervision Conditions IEPD package for a detailed explanation of the SCS data model.

5.2.2 Data Outputs

All actions of the service return a synchronous WS-RM-based *acknowledgement* or *fault* message. The acknowledgement message indicates that the input message was successfully received and provides identifiers that can be used to correlate an asynchronous response to the original input message. The fault message indicates that the request message could not be processed, including the reason for the failure.

5.2.3 Data Provenance

The data exchange by this service originates at the Responding System. The provenance of the data will be restricted to the data provided by the specific responding partner agency.

5.3 Behavior Model

5.3.1 Action Model

Included in this section are the actions defined by the SCS Service.

Action Name	SupervisionConditionsQuery
Action Purpose	
Consumer systems invoke this action to submit a request message to the service.	
Action Inputs	Action Outputs
SupervisionConditionsQueryMessage	WS-RM acknowledgement or fault
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

Action Name	SupervisionConditionsResponse
Action Purpose	
Provider systems invoke this action to submit an asynchronous response message to the service.	
Action Inputs	Action Outputs
SupervisionConditionsResponseMessage	WS-RM acknowledgement or fault
Action Provenance	
The provenance of this action is the same as the provenance of the service.	

5.3.2 Process Model

The information flow diagram, sequence diagram, and business process modeling notation (BPMN) diagram provided below further describe the behavior model of the service. These diagrams are also included in the [artifacts/service model/behavior model](#) folder of the Service Specification Package for reference.

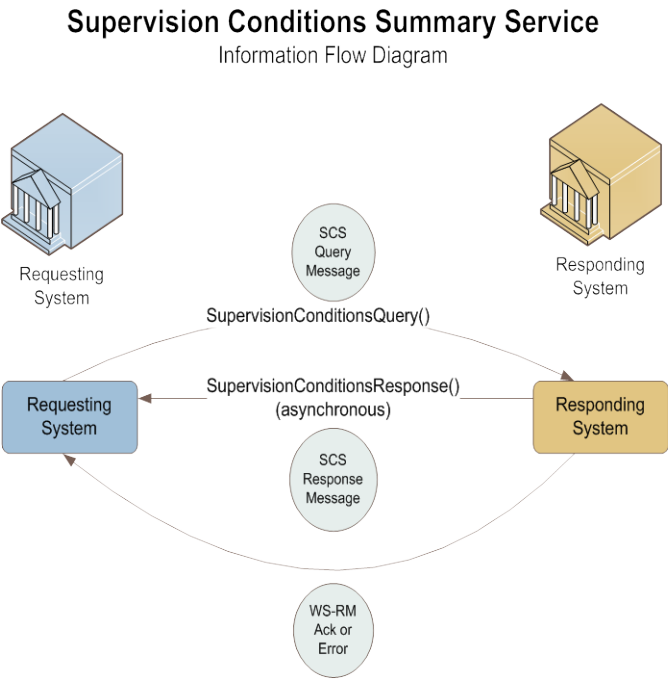


Figure 2: Information Flow Diagram

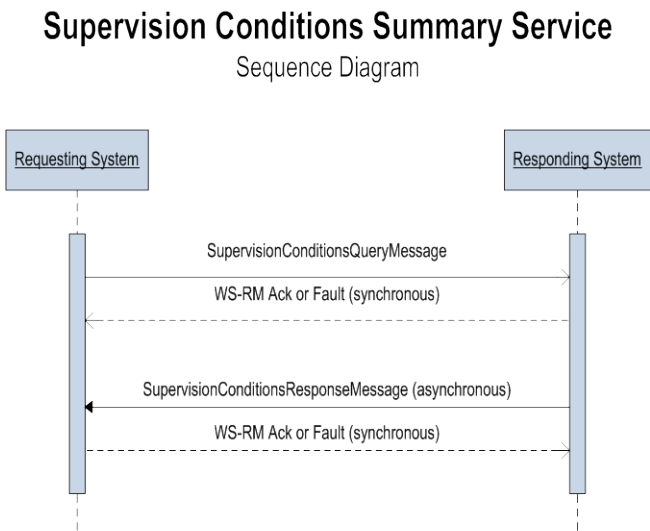


Figure 3: Sequence Diagram

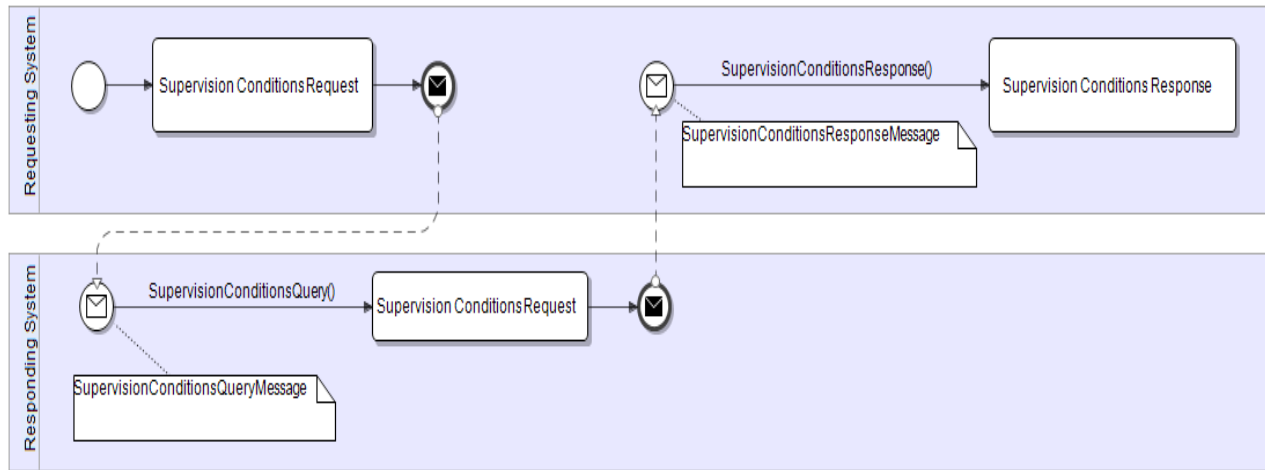


Figure 4: BPMN Diagram

Appendix A—References

Global Reference Architecture Web site	http://www.it.ojp.gov/globalgra
CJIS Security Policy	The CJIS Security Policy is considered to be Sensitive But Unclassified (SBU) material. This policy may not be posted to a public Web site, and discretion must be exercised in sharing the contents of the policy with individuals and entities who are not engaged in law enforcement or the administration of criminal justice. A copy may be obtained by contacting the state's CJIS Systems Officer (CSO).

Appendix B—Glossary

APPA	American Probation and Parole Association
BPMN	Business Process Modeling Notation
SCS	Supervision Conditions Summary
SBU	Sensitive But Unclassified
WS-RM	Web Services Reliable Messaging

Appendix C—Document History

Date	Version	Editor	Change
04/11/2011	0.9.0	Collin Evans	Initial version
07/21/2011	1.0.0	Collin Evans	Updates per SSG 1.0.0
04/11/2012	1.0.0	David Gillespie	Global Advisory Committee approved

About Global

www.it.ojp.gov/global

The Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

For more information on Global and its products, including those referenced in this document, call (850) 385-0600 or visit <http://www.it.ojp.gov/GIST>.

About GSC

www.it.ojp.gov/gsc

In accordance with the founding principle of Global, the Global Standards Council (GSC) directly supports the broadscale exchange of pertinent justice and public safety information by promoting standards-based electronic information exchanges for the justice community as a whole. Specifically, the GSC develops, maintains, and sustains the standards—including this particular standard—associated with these aforementioned information exchanges. To further foster community participation and reuse, the GSC also receives, evaluates, and recommends to Global for adoption proposed standards submitted by Global consumers and stakeholders. In turn, the GSC employs an enterprise architecture approach for developing and maintaining the cohesive body of Global standards as one Global Standards Package (GSP), which can be accessed at <http://www.it.ojp.gov/gsp>.

<http://www.it.ojp.gov/gsp>
