Quick Reference Guide

NIST Special Publication 800-53 Reference Database Application

This is a quick reference guide for the NIST Special Publication 800-53 reference database application. The database contains the catalog of security controls described in NIST Special Publication 800- 53, *Recommended Security Controls for Federal Information Systems* (the complete document is available from the NIST web site at http://csrc.nist.gov/sec-cert). The database application has been developed primarily to help our customers quickly and efficiently:

- ***Browse*** the security controls, control enhancements, and supplemental guidance contained in NIST Special Publication 800-53;
- ***Search*** the security control catalog using user-specified keywords; and
- ***Export*** security control-related information in the database application to other popular data formats that can be used in various tools and applications employed by agencies. Please note that the information in the database is *read only* and can be viewed or extracted, but cannot be updated or modified using this application.

Getting Started—

Ensure that the database application has been successfully installed. Follow the installation instructions provided in the **Readme.txt** file that was provided in the initial set of files downloaded from the NIST web site at http://csrc.nist.gov/sec-cert.

Modes of Operation

The **Browse** and **Find** modes found in the drop-down list of the "View" tab on the top menu bar are the recommended/supported modes of operation in the Beta release of the database application. The **Browse** mode allows users to navigate the different views or layouts and review each control represented as a record. The **Layout** button in the menu area of the header displays the current activated view or layout operation from the SP 800-53 Home navigation page. The drop-down menu of the **Layout** button lists the view or layout operations and by selecting and clicking on the desired operation will activate that view or layout operation. The **Find** mode puts the application in the search state where users can look for specific records in the database based on selected search criteria. Clicking the **Start New Search** button also puts the application into the **Find** mode. Clicking on the **Home** button returns the application to the **Browse** mode.

Application Functionality

From the home page of the database application, you can do any of the following operations:

Option 1: Browsing the Security Control Catalog

To ***Browse*** the security control catalog and view the controls, control enhancements, and supplemental guidance, place the cursor over any of the hot-linked areas on the home page and click one time to obtain the requested view of the control catalog.

The **Management Control Class – Summary** view displays all of the management controls in the Special Publication 800-53 control catalog by control baseline.

The **Operational Control Class – Summary** view displays all of the operational controls in the Special Publication 800-53 control catalog by control baseline.

The **Technical Control Class – Summary** view displays all of the technical controls in the Special Publication 800-53 control catalog by control baseline.

For a more refined view of the security controls in a particular **family**, place the cursor over any family within the management, operational, and technical control classes, and click one time to display all of the controls in the selected family by control baseline.

To obtain specific information about a particular **security control** in the control catalog, place the cursor over the unique identifier for the desired control (e.g., CA-2, IA-5, CP-8), and click one time to display the control information.

The **Minimum Security Controls – Summary** view displays all security controls in all baselines simultaneously.

The **Low-Impact Controls** view provides a more refined view of the security control catalog displaying only those controls in the low baseline.

The **Moderate-Impact Controls** view provides a more refined view of the security control catalog displaying only those security controls in the moderate baseline.

The **High-Impact Controls** view provides a more refined view of the security control catalog displaying only those security controls in the high baseline.

The **Security Controls Catalog** view provides access to the individual security controls. Clicking on the right or left arrows in the "binder" icon in the menu area of the left margin moves forward or backward sequentially through the control catalog displaying the detailed information for each control. The scroll mechanism on the information system mouse can also be used to move forward or backward through the control catalog.

The **Record** section in the menu area of the header displays the current record number of the total records **Found** in the selected view of the control catalog. The **Total** section lists the total number of records in the database which corresponds to the total number of security controls in the control catalog.

Clicking the **Home** button on the top menu bar returns to the database application to the main screen in the application.

Clicking the **Control** button on the top menu of any **Management**, **Operational**, or **Technical**, **Class Summary** view or **Minimum Security Controls Summary** view provides access to the individual security controls from the current view (e.g., **management control class – summary** view, **media protection family** view).

Option 2: Searching the Security Control Catalog

To ***search*** the security control catalog, place the cursor over the **Start New Search** button near the bottom of the home page and click one time to activate the search engine. A blank template will be displayed allowing the user to input keywords or criteria in any of the sections where the desired search is to be initiated. Once the criteria are entered, click the **Find** button located in the left margin to begin the search. In the current implementation, the application supports three search modes: single keyword searches, AND searches, and OR searches.

- To find an occurrence of a keyword or multiple keywords in a specific field, click the **Start New Search** button, enter the keyword in the desired field and click the **Find** button in the left margin or press the **Enter** key to perform the search.
- To find an occurrence of a keyword in two or more specific fields, click the **Start New Search** button; enter the keyword in the first, second, and any subsequent desired fields. Click the **Find** button or press the **Enter** key to perform the search.
- To find an occurrence of a keyword in any of the specific fields, click the **Start New Search** button, enter the keyword in the first desired field, click the **New Criteria – OR Searches** button to create a new blank template, enter the keyword in the second desired field and repeat the last

two steps for each additional desired field. Click the **Find** button or press the **Enter** key to perform the search. Note that the **New Criteria - OR Searche**s button will only work in the **Find** mode or after the **Start New Search** button is activated.

Upon completion of the search, the **Record** section in the left margin indicates which occurrence (i.e., security control) is currently being displayed and the **Found** section indicates the number of occurrences returned during the search. The left and right arrows in the "binder" icon in the menu area of the left margin moves forward or backward sequentially through individual occurrences found during the search. The scroll mechanism on the information system mouse can also be used to move forward or backward through the control catalog.

Option 3: Exporting Security Control-Related Information from the Control Catalog

To export security control-related information from the control catalog, place the cursor over the **export** button near the bottom of the home page and click one time to activate the export function. A window will be displayed which will allow the user to specify the type of file format to be used during the export operation and the directory where the exported information is to be placed. By default, all data fields are exported. The user can choose the fields that are exported by selecting the name of field and click **move** or remove the field by highlighting it in the field export order box and click **clear**. Once the data is exported, the user can use a third party application (e.g., spreadsheet or database), to import the data in order to customize or tailor it. The following table lists all the data fields that are defined in the SP 800-53 Reference Database Application.

FIELD NAME	DATA TYPE	SAMPLE DATA
Family	Text	SYSTEM AND COMMUNICATIONS PROTECTION
Class	Text	TECHNICAL
Family of Control	Text	SC-
Control Number	Number	7
Control Name	Text	BOUNDARY PROTECTION
Control	Text	The information system: a. Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and b. Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
Supplemental Guidance	Text	Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a

		demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.
Ctrl Enh Num 1	Text	(1)
Control Enhancements 1	Text	The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.
Enhancement Supplemental Guidance 1	Text	Publicly accessible information system components include, for example, public web servers.
Ctrl Enh Num 2	Text	(2)
Control Enhancements 2	Text	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.
Enhancement Supplemental Guidance 2	Text	
Ctrl Enh Num 3	Text	(3)
Control Enhancements 3	Text	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.
Enhancement Supplemental Guidance 3	Text	The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.
Ctrl Enh Num 4	Text	(4)
Control Enhancements 4	Text	The organization: (a) Implements a managed interface for each external telecommunication service; (b) Establishes a traffic flow policy for each managed interface;

		(c) Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted; (d) Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need; (e) Reviews exceptions to the traffic flow policy [Assignment: organization-defined frequency]; and (f) Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.
Enhancement Supplemental Guidance 4	Text	
Ctrl Enh Num 5	Text	(5)
Control Enhancements 5	Text	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).
Enhancement Supplemental Guidance 5	Text	
Ctrl Enh Num 6	Text	(6)
Control Enhancements 6	Text	The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.
Enhancement Supplemental Guidance 6	Text	
Ctrl Enh Num 7	Text	(7)
Control Enhancements 7	Text	The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.
Enhancement Supplemental Guidance 7	Text	This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources

		such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.
Ctrl Enh Num 8	Text	(8)
Control Enhancements 8	Text	The information system routes [Assignment: organization-defined internal communications traffic] to [Assignment: organization-defined external networks] through authenticated proxy servers within the managed interfaces of boundary protection devices.
Enhancement Supplemental Guidance 8	Text	External networks are networks outside the control of the organization. Proxy servers support logging individual Transmission Control Protocol (TCP) sessions and blocking specific Uniform Resource Locators (URLs), domain names, and Internet Protocol (IP) addresses. Proxy servers are also configurable with organization-defined lists of authorized and unauthorized websites.
Ctrl Enh Num 9	Text	(9)
Control Enhancements 9	Text	The information system, at managed interfaces, denies network traffic and audits internal users (or malicious code) posing a threat to external information systems.
Enhancement Supplemental Guidance 9	Text	Detecting internal actions that may pose a security threat to external information systems is sometimes termed extrusion detection. Extrusion detection at the information system boundary includes the analysis of network traffic (incoming as well as outgoing) looking for indications of an internal threat to the security of external systems.
Ctrl Enh Num 10	Text	(10)
Control Enhancements 10	Text	The organization prevents the unauthorized exfiltration of information across managed interfaces.
Enhancement Supplemental Guidance 10	Text	Measures to prevent unauthorized exfiltration of information from the information system include, for example: (i) strict adherence to protocol formats; (ii) monitoring for indications of beaconing from the information system; (iii) monitoring for use of steganography; (iv) disconnecting external network interfaces except when explicitly needed; (v) disassembling and reassembling packet headers; and (vi) employing traffic profile analysis to detect

		deviations from the volume or types of traffic expected within the organization. Examples of devices enforcing strict adherence to protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification at the application layer and serve to identify vulnerabilities that cannot be detected by devices operating at the network or transport layer.
Ctrl Enh Num 11	Text	(11)
Control Enhancements 11	Text	The information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination.
Enhancement Supplemental Guidance 11	Text	
Ctrl Enh Num 12	Text	(12)
Control Enhancements 12	Text	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.
Enhancement Supplemental Guidance 12	Text	A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.
Ctrl Enh Num 13	Text	(13)
Control Enhancements 13	Text	The organization isolates [Assignment: organization defined key information security tools, mechanisms, and support components] from other internal information system components via physically separate subnets with managed interfaces to other portions of the system.
Enhancement Supplemental Guidance 13	Text	
Ctrl Enh Num 14	Text	(14)
Control Enhancements 14	Text	The organization protects against unauthorized physical connections across the boundary protections implemented at [Assignment: organization-defined list of managed interfaces].
Enhancement Supplemental Guidance 14	Text	Information systems operating at different security categories may routinely share common physical and environmental controls, since the systems may share space within organizational facilities. In practice, it is possible that these separate information systems may share common

		equipment rooms, wiring closets, and cable distribution paths. Protection against unauthorized physical connections can be achieved, for example, by employing clearly identified and physically separated cable trays, connection frames, and patch panels for each side of managed interfaces with physical access controls enforcing limited authorized access to these items. Related control: PE-4.
Ctrl Enh Num 15	Text	(15)
Control Enhancements 15	Text	The information system routes all networked, privileged accesses through a dedicated, managed interface for purposes of access control and auditing.
Enhancement Supplemental Guidance 15	Text	Related controls: AC-2, AC-3, AC-4, AU-2.
Ctrl Enh Num 16	Text	(16)
Control Enhancements 16	Text	The information system prevents discovery of specific system components (or devices) composing a managed interface.
Enhancement Supplemental Guidance16	Text	This control enhancement is intended to protect the network addresses of information system components that are part of the managed interface from discovery through common tools and techniques used to identify devices on a network. The network addresses are not available for discovery (e.g., not published or entered in the domain name system), requiring prior knowledge for access. Another obfuscation technique is to periodically change network addresses.
Ctrl Enh Num 17	Text	(17)
Control Enhancements 17	Text	The organization employs automated mechanisms to enforce strict adherence to protocol format.
Enhancement Supplemental Guidance 17	Text	Automated mechanisms used to enforce protocol formats include, for example, deep packet inspection firewalls and XML gateways. These devices verify adherence to the protocol specification (e.g., IEEE) at the application layer and serve to identify significant vulnerabilities that cannot be detected by devices operating at the network or transport layer.
Control Enhancements 18	Text	(18)
Ctrl Enh Num 18	Text	The information system fails securely in the event of an operational failure of a boundary protection device.
Enhancement Supplemental Guidance 18	Text	Fail secure is a condition achieved by the application of a set of information system

		mechanisms to ensure that in the event of an operational failure of a boundary protection device at a managed interface (e.g., router, firewall, guard, application gateway residing on a protected subnetwork commonly referred to as a demilitarized zone), the system does not enter into an unsecure state where intended security properties no longer hold. A failure of a boundary protection device cannot lead to, or cause information external to the boundary protection device to enter the device, nor can a failure permit unauthorized information release.
References	Text	FIPS Publication 199; NIST Special Publications 800-41, 800-77.
Priority Code	Text	P1
Low	Text	LOW
Low Ctrl Name	Text	SC-
Low Ctrl Num	Text	7
Low Ctrl Enh Num	Text	
Moderate	Text	MOD
Mod Ctrl Name	Text	SC-
Mod Ctrl Num	Text	7
Mod Ctrl Enh Num	Text	(1) (2) (3) (4) (5) (7)
High	Text	HIGH
High Ctrl Name	Text	SC-
High Ctrl Num	Text	7
High Ctrl Enh Num	Text	(1) (2) (3) (4) (5) (6) (7) (8)