



## FISMA – Bsafe Road Map

This document presents a list of FISMA controls taken from Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems and matches to each the features of Bsafe/Enterprise Security which address the requirements outlined.

### **FISMA Minimum Assurance Requirements**

Appendix E of the FISMA Special Publication 800-53 describes three different security control baselines (low, moderate and high).

The low baseline requires assurance that the appropriate controls are in effect. The moderate baseline requires, in addition to the demand of the low baseline, detailed description of the control which will permit analysis and testing of the control.

The high baseline goes a step further. It requires, in addition to the demand of the moderate baseline, a complete implementation including administrator interface, clear operating instructions, any supporting applications necessary. It must be able to be proved rugged and reliable.

Bsafe/Enterprise Security and related Bsafe products fall into the category of the high baseline assurance requirements for many of the listed controls. They are independent of specific user applications, being fully documented, with an integrated administrator interface. They are off-the-shelf products working in many different environments, not application-specific developments.



**FISMA Security Control Catalog**

Appendix F of the FISMA Special Publication 800-53 details a range of safeguards, or controls, for information systems. The following tables map these controls to Bsafe/Enterprise Security functionality.

Access Control - AC

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>AC-1</b>	<p><b>Access Control Policy and Procedures:</b></p> <ul style="list-style-type: none"> <li>• Formal, documented, access control policy</li> <li>• Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls</li> </ul>	<p><b>Application Access Control</b> Permissions templates.</p> <p><b>Policy Compliance Manager</b> IP Filtering compliance policy, User profile compliance policy, object authority compliance policy, system values compliance policy.</p> <p><b>IP Packet Lockdown</b> Policy definitions.</p>
<b>AC-2</b>	<p><b>Account Management</b> Management of information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.</p> <p>+ <b>Control Enhancements</b> for more details</p>	<p><b>User Profile Manager</b> Simplified user control.</p> <p><b>Policy Compliance Manager</b> User profile compliance policy.</p>
<b>AC-3</b>	<p><b>Access Enforcement</b></p> <p><b>Control Enhancements</b> Explicitly authorized personnel</p>	<p><b>Application Access Control</b> At user and various user group levels for network and other exit program controlled access and usage.</p>
<b>AC-4</b>	<p><b>Information Flow Enforcement</b> (between computers in or outside of the network)</p>	<p><b>Application Access Control</b> At the IP address and remote system name level.</p> <p><b>IP Packet Lockdown</b> Control of traffic to and from specified sources and destinations.</p>



Control	Description	Bsafe/Enterprise Security Controlling Function
AC-5	<p><b>Separation of Duties</b> Separation of duties through assigned access authorizations.</p> <p>+ <b>Supplemental Guidance</b> for more details:</p>	<p><b>Administrator Role Manager</b> Administration access by role.</p> <p><b>Application Access Control</b> At user and various user group levels for selected applications and functions.</p>
AC-6	<p><b>Least Privilege</b> The most restrictive set of rights/privileges or accesses needed by users</p>	<p><b>Application Access Control</b> Priority Level: User ID / group profile, generic name / Bsafe Group / IP Address / System Policy.</p>
AC-7	<p><b>Unsuccessful Login Attempts</b> Limit of consecutive invalid access attempts by a user</p>	<p><b>System Audit</b> Audit Policy for unsuccessful logins.</p> <p><b>Application Audit</b> Inquiries, reports and graphs of unsuccessful login events.</p> <p><b>Alert Center</b> Action following defined number of failed login attempts.</p>
AC-8	<p><b>System Use Notification (partial)</b> Message informing users their work will be monitored. Required acceptance by the user before continuing</p>	<p><b>Screen Capture</b> Forces users to confirm their acceptance of monitoring before being allowed to continue working.</p>
AC-9	Previous Logon Notification	N/A
AC-10	<p><b>Concurrent Session Control</b> Limit of the number of concurrent sessions for a user</p>	<p><b>Application Access Control</b> Telnet device file name control allows one or more display device names to be specified Restriction of command TFRSECJOB to control use of system request function to open a new session.</p>
AC-11	<b>Session Lock</b>	<b>Session Timeout</b>



Control	Description	Bsafe/Enterprise Security Controlling Function
	Organization-defined time periods of inactivity at system policy, user and user group level.	Control of idle-time allowed and action to take. Can be tailored to the needs of different users and groups.
AC-12	<b>Session Termination</b> As for AC-11, above	<b>Session Timeout</b> As for AC-11, above
AC-13	<b>Supervision and Review—Access Control</b> Reviews of audit records (e.g., user activity logs) for inappropriate activities in accordance with organizational procedures.	<p><b>Application Audit</b> On-line review and printed reports of network access and other exit program activity with rich filtering capabilities</p> <p><b>Application Analyzer</b> Dynamic graphs based on application audit data, presented in dynamically-defined paths</p> <p><b>Cross-Platform Audit</b> Consolidation of audit data from different computers, even different platforms</p> <p><b>System Audit</b> Comprehensive audit of system events</p> <p><b>Alert Center</b> Instant alerts following unauthorized access events with a wide selection of actions</p>
AC-14	Permitted Actions without Identification or Authentication	N/A
AC-15	Automated Marking	N/A
AC-16	Automated Labeling	N/A
AC-17	<b>Remote Access</b> Authorization, monitoring, and control of all methods of remote access to the information system.	<p><b>Application Access Control</b> See above</p> <p><b>Application Audit</b> See above</p>
AC-18	Wireless Access Restrictions	N/A



Control	Description	Bsafe/Enterprise Security Controlling Function
AC-19	Access Control for Portable and Mobile Devices	N/A
AC-20	Use of External Information Systems	N/A

Awareness and Training – AT: N/A

Audit and Accountability - AU

Control	Description	Bsafe/Enterprise Security Controlling Function
AU-1	<p><b>Audit and Accountability Policy and Procedures</b></p> <p>(i) A formal, documented policy</p> <p>(ii) Formal, documented procedures to facilitate the implementation of the policy</p>	<p><b>Application Audit</b> Permissions templates for users, groups of users, IP addresses and system</p> <p><b>System Audit Policy Manager</b> Definition of system events to be audited at the system, user and object levels</p> <p><b>Policy Compliance Manager</b> System values compliance policy</p> <p><b>Central Audit</b> Read-data policy – specifying files to monitor for data records read.</p>
AU-2	<b>Auditable Events</b>	<p><b>Application Audit</b> On-line review and printed reports of network access and other exit program activity with rich filtering capabilities</p> <p><b>Application Analyzer</b> Dynamic graphs based on application audit data, presented in dynamically-defined paths</p> <p><b>Cross-Platform Audit</b></p>



Control	Description	Bsafe/Enterprise Security Controlling Function
		<p>Consolidation of audit data from different computers, even different platforms</p> <p><b>System Audit</b> Comprehensive audit of system events</p> <p><b>Alert Center</b> Instant alerts following unauthorized access events with a wide selection of actions</p> <p><b>Central Audit</b> Read data, IP packet, Admin Audit</p>
<p><b>AU-3</b></p>	<p><b>Content of Audit Records</b> Audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events (including date, time, system component, where occurred, user, success/failure status.</p> <p>Enhancements</p> <ol style="list-style-type: none"> <li>1. More detailed information</li> <li>2. Central management of audit records</li> </ol>	<p>As for AU-2, above</p>
<p><b>AU-4</b></p>	<p><b>Audit Storage Capacity</b> Allocation of sufficient audit record storage capacity and configuration of auditing to reduce the likelihood of such capacity being exceeded.</p>	<p><b>Cross-Platform Audit and Central Audit</b> Allow importing of selected audit information for long-term storage.</p> <p>Cross-Platform Audit data is stored on dedicated server. This allows removal of audit data from source computers.</p>
<p><b>AU-5</b></p>	<p><b>Response to Audit Processing Failures</b></p>	<p><b>Alert Center</b> Instant alerts following any</p>



Control	Description	Bsafe/Enterprise Security Controlling Function
	<p>Alerting of appropriate organizational officials in the event of an audit processing failure and the taking of additional actions:</p> <p>Enhancements</p> <ol style="list-style-type: none"> <li>1. warning when maximum audit record storage reached</li> <li>2. Real-time alert</li> </ol>	<p>system audit event</p> <p>Application audit alert if Maximum storage reached (for entire system).</p> <p>Alerts if Bsafe audit log(s) Application Audit, Central Audit and Cross Platform audit maximum size reached</p>
<p><b>AU-6</b></p>	<p><b>Audit Monitoring, Analysis, and Reporting</b></p> <p>Regular review/analysis of information system audit records for indications of inappropriate or unusual activity</p> <p>Enhancements</p> <ol style="list-style-type: none"> <li>1. Automated mechanisms to integrate audit monitoring, analysis, and reporting into an overall process.</li> <li>2. Real-time alerts</li> </ol>	<p><b>Application Audit Alert Center</b></p> <p><b>Application Analyzer</b></p> <p>This control is a human procedural control. However, it can be facilitated by the built-in graphs and analysis tools.</p> <p>Reports can be scheduled for regular runs.</p> <p>Alert Center can trigger alerts on all events.</p>
<p><b>AU-7</b></p>	<p><b>Audit Reduction and Report Generation</b></p> <p>An audit reduction and report generation capability.</p> <p>Enhancements</p> <ol style="list-style-type: none"> <li>1. Automated processing of records based on selection criteria</li> </ol>	<p><b>Report Generator</b></p> <p><b>System Audit Reports</b></p> <p><b>Application Audit Reports</b></p> <p><b>CPA and Central Audit reports</b></p> <p>All of the above reporting features include scheduling options and filtering of criteria.</p>
<p><b>AU-8</b></p>	<p><b>Time Stamps</b></p> <p>For use in audit record generation</p>	<p>Included in all logged events and alerts</p>



Control	Description	Bsafe/Enterprise Security Controlling Function
<p><b>AU-9</b></p>	<p><b>Protection of Audit Information</b> Protection of audit information and audit tools from unauthorized access, modification, and deletion.</p>	<p>Two-level authentication – server user and Bsafe/Enterprise Security Application.</p> <p>All data stored on secure System i server (except CPA). Files protected by being security officer owned.</p> <p>Additional option – file protection facility</p>
<p><b>AU-10</b></p>	<p><b>Non-repudiation</b> The capability to determine whether a given individual took a particular action</p>	<p><b>System audit, Application audit, Read-data audit file audit</b> Actions are logged with user ID.</p>
<p><b>AU-11</b></p>	<p><b>Audit Record Retention</b> Retaining of audit records for a defined time period for after-the-fact investigations of security incidents</p>	<p><b>CPA and Central audit</b> Allow selective retention for unlimited terms.</p>



Certification, Accreditation and Security Assessments - CA

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>CA-1</b>	Certification, Accreditation, and Security Assessment Policies and Procedures	N/A
<b>CA-2</b>	<b>Security Assessments</b> The conducting of an assessment of the security controls in the information system	<b>Bsafe/Security Assessment Tool</b>  <b>Policy Compliance Manager</b>
<b>CA-3</b>	Information System Connections	N/A
<b>CA-4</b>	Security Certification	N/A
<b>CA-5</b>	Plan of Action and Milestones	N/A
<b>CA-6</b>	Security Accreditation	N/A
<b>CA-7</b>	Continuous Monitoring	N/A

Configuration Management - CM

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>CM-1</b>	Configuration Management Policy and Procedures	N/A
<b>CM-2</b>	<b>Baseline Configuration</b> A current baseline configuration of the information system.	<b>Policy Compliance Manager</b>
<b>CM-3</b>	Configuration Change Control	N/A
<b>CM-4</b>	<b>Monitoring Configuration Changes</b> The monitoring of changes to the information system	<b>Policy Compliance Manager</b>  <b>System Audit</b>



<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>CM-5</b>	<b>Access Restrictions for Change</b>	<b>Bsafe administrator audit (in Central Audit)</b>  <b>Administration Role Manager</b>
<b>CM-6</b>	<b>Configuration Settings</b> Documentation and implementation of mandatory configuration settings	<b>Policy Compliance Manager</b>
<b>CM-7</b>	<b>Least Functionality</b> Allowing only essential capabilities and prohibiting and/or restricting the use of the functions, ports, protocols, and/or services	<b>Application Access Control</b>  <b>Administration Role Manager</b>
<b>CM-8</b>	Information System Component Inventory	N/A

Contingency Planning - CM  
N/A

Identification and Authentication - IA

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>IA-1</b>	<b>Identification and Authentication Policy and Procedures</b>	<b>Security Assessment Tool</b> for password system values.  <b>Policy Compliance Manager</b> for User ID and password system values
<b>IA-2</b>	User Identification and Authentication	N/A
<b>IA-3</b>	<b>Device Identification and Authentication</b> Identification and authentication of specific devices (by TCP/IP addresses or other means) before establishing a connection.	<b>Application Access Control</b> Telnet device file restrictions, IP address restrictions for Telnet, FTP, database server, DDM



Control	Description	Bsafe/Enterprise Security Controlling Function
IA-4	<b>Identifier Management</b> Including disabling the user identifier after a defined period of inactivity	Assisted by <b>User Profile Manager</b>  <b>Inactive User Manager</b>  <b>Session Timeout</b>
IA-5	<b>Authenticator Management</b> Management of information system authenticators e.g. password regeneration, password policy control, other	<b>User Profile Manager:</b> generation of new default passwords and sending by email, setting password to expired.  <b>Policy Compliance Manager:</b> enforcement of password system values, enforcement of user profile parameters
IA-6	Authenticator Feedback	N/A
IA-7	Cryptographic Module Authentication	N/A

Incident Response - IR

Control	Description	Bsafe/Enterprise Security Controlling Function
IR-1	<b>Incident Response Policy and Procedures</b> Formal, documented incident policy and procedures	<b>Alert Center.</b> Alerts can be defined and reviewed. Wide scope in defining triggering circumstances and resulting actions
IR-2	<b>Incident Response Training</b> Training for incident response	See above. Warning mode facilitates training.
IR-3	<b>Incident Response Testing and Exercises</b> Testing the incident response capabilities	See above. Warning mode facilitates testing.
IR-4	<b>Incident Handling</b>	See above. Wide scope of actions following an alert including messaging, automatic program execution and disabling



Control	Description	Bsafe/Enterprise Security Controlling Function
		of users
<b>IR-5</b>	<b>Incident Monitoring</b>	<b>Alert Center</b> <b>Application Audit</b> <b>Application Analyzer (graphs)</b> <b>System Audit</b> <b>Central Audit</b>
<b>IR-6</b>	<b>Incident Reporting</b>	<b>Application Audit</b> reports
<b>IR-7</b>	<b>Incident Response Assistance</b>	Integrated environment for auditing, permissions definitions and user management provides a wide picture to personnel handling incident response.

Maintenance - MA

Control	Description	Bsafe/Enterprise Security Controlling Function
<b>MA-1</b>	System Maintenance Policy and Procedures	N/A
<b>MA-2</b>	Controlled Maintenance	N/A
<b>MA-3</b>	<b>Maintenance Tools</b>	<b>Report Generator, System reports and SAT (Security Assessment Tool)</b> to review authorities to maintenance system commands
<b>MA-4</b>	<b>Remote Maintenance</b>	<b>Application Access Control</b> to restrict access
<b>MA-5</b>	<b>Maintenance Personnel</b>	As for MA-3, MA-4 above
<b>MA-6</b>	Timely Maintenance	N/A

Media Protection - MP

N/A

Physical and Environmental Protection - PE

N/A

Planning - PL

N/A



Personnel Security - PS  
N/A

Risk Assessment - RA

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>RA-1</b>	Risk Assessment Policy and Procedures	N/A
<b>RA-2</b>	Security Categorization	N/A
<b>RA-3</b>	<b>Risk Assessment</b> Including vulnerabilities, threat sources, and security controls planned or in place	<b>Bsafe Security Assessment Tool (SAT), Policy Compliance Managet</b>
<b>RA-4</b>	<b>Risk Assessment Update</b>	<b>Policy Compliance Manager</b>
<b>RA-5</b>	<b>Vulnerability Scanning</b>	<b>Bsafe Security Assessment Tool (SAT), Policy Compliance Manage</b>

Systems and Services Acquisition - SA  
N/A

System and Communications Protection – SC

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>SC-1</b>	<b>System and Communications Protection Policy and Procedures</b>	N/A
<b>SC-2</b>	<b>Application Partitioning</b>	
<b>SC-3</b>	<b>Security Function Isolation</b> The isolation of security functions from nonsecurity functions.	<b>Administration Role Manager</b> to give different administrators and auditors different powers.. <b>Application Access Control</b> to restrict access to selected functionality
<b>SC-4</b>	Information Remnance	N/A
<b>SC-5</b>	Denial of Service Protection	N/A
<b>SC-6</b>	Resource Priority	N/A



<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>SC-7</b>	<b>Boundary Protection</b>	<b>Application Access Control</b>
<b>SC-8</b>	<b>Transmission Integrity</b>	SSL encryption between Bsafe/Enterprise Security Manager and server software
<b>SC-9</b>	Transmission Confidentiality	N/A
<b>SC-10</b>	<b>Network Disconnect</b>	<b>Session Timeout</b>
<b>SC-11</b>	Trusted Path	N/A
<b>SC-12</b>	Cryptographic Key Establishment and Management	N/A
<b>SC-13</b>	Use of Cryptography	N/A
<b>SC-14</b>	Public Access Protections	N/A
<b>SC-15</b>	Collaborative Computing	N/A
<b>SC-16</b>	Transmission of Security Parameters	N/A
<b>SC-17</b>	Public Key Infrastructure Certificates	N/A
<b>SC-18</b>	Mobile Code	N/A
<b>SC-19</b>	Voice Over Internet Protocol	N/A
<b>SC-20</b>	Secure Name /Address Resolution Service (Authoritative Source)	N/A
<b>SC-21</b>	Secure Name /Address Resolution Service (Recursive or Caching Resolver)	N/A
<b>SC-22</b>	Architecture and Provisioning for Name/Address Resolution Service	N/A
<b>SC-23</b>	Session Authenticity	N/A

System and Information Integrity – SI

<b>Control</b>	<b>Description</b>	<b>Bsafe/Enterprise Security Controlling Function</b>
<b>SI-1</b>	System and Information Integrity Policy and Procedures	N/A
<b>SI-2</b>	Flaw Remediation	N/A
<b>SI-3</b>	<b>Malicious Code Protection</b> malicious code protection mechanisms at critical information system entry and exit points	<b>Application Access Control</b> File Server protection controls access to IFS where malicious programs could be dispersed



Control	Description	Bsafe/Enterprise Security Controlling Function
<p><b>SI-4</b></p> <p><b>Information System Monitoring Tools and Techniques</b></p> <p>Tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system.</p>		<p><b>Application Audit</b>  <b>Read Data, System Audit</b></p>
<p><b>SI-5</b></p>	<p>Security Alerts and Advisories</p>	<p>N/A</p>
<p><b>SI-6</b></p>	<p><b>Security Functionality Verification</b></p> <p>Verification of the correct operation of security functions including notification where necessary</p>	<p><b>Policy Compliance Manager,</b>  <b>Security Assessment Tool,</b>  <b>System Audit</b></p>
<p><b>SI-7</b></p>	<p><b>Software and Information Integrity</b></p> <p>Detection and protection against unauthorized changes to software and information</p>	<p><b>File Audit, Application Access Control, Object Authority Manager, SOX Compliance Alerts, SOX Compliance Reports</b></p>
<p><b>SI-8</b></p>	<p>Spam Protection</p>	<p>N/A</p>
<p><b>SI-9</b></p>	<p><b>Information Input Restrictions</b></p> <p>Restricts the capability to input information to the information system to authorized personnel.</p>	<p>Field Masking, File Protection</p>
<p><b>SI-10</b></p>	<p>Information Accuracy, Completeness, Validity, and Authenticity</p>	<p>N/A</p>
<p><b>SI-11</b></p>	<p>Error Handling</p>	<p>N/A</p>
<p><b>SI-12</b></p>	<p>Information Output Handling and Retention</p>	<p>N/A</p>



For more information:

Visit our website,  
[www.bsafesolutions.com](http://www.bsafesolutions.com)

Call one of our offices,

<b>USA New Jersey</b>	Tel: 877-237-8024 toll free	<a href="mailto:salesusa@bsafesolutions.com">salesusa@bsafesolutions.com</a>
<b>Canada</b>	Tel: 905-9434042	<a href="mailto:info-ca@bsafesolutions.com">info-ca@bsafesolutions.com</a>
<b>Europe &amp; R.O.W.</b>	Tel: +972-9-9610400	<a href="mailto:info-eu@bsafesolutions.com">info-eu@bsafesolutions.com</a>

Or speak to a local reseller near you. See the list on our website

## Maximum Security, **Simply!**

© Copyright 2008 Bsafe Information Systems, Ltd. All rights reserved. This document is the property of Bsafe Information Systems, Ltd. It cannot be passed on to any party, individual or organization without the express permission of Bsafe Information Systems. [www.bsafesolutions.com](http://www.bsafesolutions.com)