

## Mapping EventTracker Reports and Alerts To FISMA Requirements

© Prism Microsystems, August 2008

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
Access Control	<b>AC-2 Account Management</b>  <b>DOD: 8500.2 IAAC.1</b> <b>DCID: 6/3 4.B.2.a(3)</b>	<ul style="list-style-type: none"> <li>• *Security: User Account disabled</li> <li>• *Security: User Account enabled</li> <li>• *Security: User Account locked</li> <li>• Active Directory: User added</li> <li>• Active Directory: User deleted</li> <li>• *Security: User added to group</li> <li>• *Security: User removed from group</li> <li>• *Security: Account rename</li> <li>• Solaris BSM: User management</li> <li>• Solaris BSM: Disable user</li> </ul>	<ul style="list-style-type: none"> <li>• Domain policy changed</li> <li>• Excessive user lockout in your enterprise</li> <li>• Excessive logon failures due to bad password/username</li> <li>• Excessive logon attempts from a particular IP address</li> <li>• Excessive access failures on a specific computer</li> <li>• Excessive access failures by a user</li> </ul>
	<b>AC-13 Supervision and Review</b>  <b>DOD: 8500.2: ECAT-1,</b> <b>ECAT-2 E3.3.9</b> <b>DCID 6/3: 2.B.7.c</b>	<ul style="list-style-type: none"> <li>• Windows: Account logon</li> <li>• Windows: Account logon failure</li> <li>• EventTracker: Initial User Network logon</li> <li>• *Security: User logon</li> <li>• *Security: User logoff</li> <li>• Active Directory: User logons</li> <li>• Active Directory: User logoffs</li> <li>• Solaris BSM: SU failure</li> <li>• Solaris BSM: Su success</li> <li>• Solaris BSM: Failed local logon/logoff</li> <li>• Solaris BSM: Privileged use</li> <li>• NetApp Data ONTAP: Delete Access</li> <li>• NetApp Data ONTAP: Logon failure</li> </ul>	<ul style="list-style-type: none"> <li>• Admin Login Failure</li> <li>• Admin Login Success</li> <li>• Solaris BSM: SU failure</li> <li>• Solaris BSM: SU success</li> <li>• Solaris BSM: User Management</li> </ul>

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
		<ul style="list-style-type: none"> <li>• NetApp Data ONTAP: Read Access</li> <li>• NetApp Data ONTAP: User Logon</li> <li>• NetApp Data ONTAP: Write Access</li> <li>• Exchange ActiveSync: Policy compliance</li> <li>• Security-&gt;Access Control (all reports)</li> </ul>	
	<p><b>AC-19 Access Control for Portable and Mobile Devices</b></p> <p>DCID 6/3    8.B.6.c</p>	<ul style="list-style-type: none"> <li>• USB Device: Report Detail</li> <li>• USB Device: Report Failure</li> <li>• Exchange ActiveSync: Policy compliance</li> <li>• Exchange ActiveSync: User Agent</li> </ul>	<ul style="list-style-type: none"> <li>• USB Insert Alert</li> </ul>
Audit And Accountability	<p><b>AU-1 Audit and Accountability Policy and Procedures</b></p> <p>8500.2: ECAT-1, ECTB-1, DCAR-1 DCID 6/3: DCID: B.2.d Manual: 2.B.4.e(5), 4.B.2.a(4)</p>	<ul style="list-style-type: none"> <li>• Active Directory: Group Policy (all reports)</li> <li>• *Security: Policy Change</li> <li>• *Security: Audit Policy change</li> <li>• Checkpoint: Audit activities</li> <li>• Solaris BSM: Audit Policy changes</li> </ul>	<ul style="list-style-type: none"> <li>• Domain Policy Changed</li> </ul>
	<p><b>AU-4 Audit Storage Capacity</b></p> <p>DCID 6/3: 5.B.2.a(5)(a)(1)</p>	<ul style="list-style-type: none"> <li>• Disk Space Forecasting: Disk Space Availability</li> <li>• Disk Space Forecasting: Disk Space Status</li> <li>• Disk Space Forecasting: Disk Utilization Trend</li> </ul>	<ul style="list-style-type: none"> <li>• Disk Full</li> <li>• Disk Space Critically Low</li> </ul>
	<p><b>AU-5 Response to Audit Process Failure</b></p> <p>DCID 6/3: 4.B.4.a(9)(d)</p>	<ul style="list-style-type: none"> <li>• EventTracker: CAB integrity verification</li> <li>• EventTracker: Collection master error</li> <li>• EventTracker: Collection point error</li> <li>• EventTracker: Disk Space low</li> <li>• EventTracker: Eventlog full</li> </ul>	<ul style="list-style-type: none"> <li>• System Audit Log Cleared</li> <li>• Critical Service Not Running</li> <li>• Critical Service Not Started</li> <li>• Event Log Full</li> <li>• Event Log Cleared</li> <li>• EventTracker agent service failed</li> </ul>

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
			<ul style="list-style-type: none"> <li>• Collection Master Error</li> <li>• Collection Point Error</li> <li>• IIS Logging Shutdown</li> <li>• MExchange: Log disk full</li> <li>• System Shutdown</li> <li>• SQL Server: Transaction Log Full</li> </ul>
	<b>AU-9 Protection Of Audit Information</b>  <b>8500.2: ECTP-1</b> <b>DCID 6/3: 4.B.2.a(4)(b)</b>	<ul style="list-style-type: none"> <li>• File Resource Access Success:Delete Access</li> <li>• File Resource Access Failure:Delete Access</li> <li>• Active Directory:Deleted Share</li> <li>• Active Directory:Share Folder deleted</li> <li>• NetApp Data ONTAP: Delete Access</li> <li>• Whatchanged: Files Deleted</li> </ul>	<ul style="list-style-type: none"> <li>• EventTracker CAB integrity checksum failed</li> <li>• Admin Login Failure</li> </ul>

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
Configuration Management	<p><b>CM-4 Monitoring Configuration Changes</b></p> <p><b>8500.2: DCPR-1, E3.3.8 DCID 6/3: 5.B.2.a(8)</b></p>	<ul style="list-style-type: none"> <li>• WhatChanged: (all reports)</li> <li>• *Security: Policy Change</li> <li>• *Security: Audit Policy Change</li> <li>• Active Directory: Changed objects</li> <li>• Active Directory: OU change</li> <li>• CISCO PIX: Priv level changed</li> <li>• EventTracker: Service changes</li> <li>• File/resource Access Failure: Change property</li> <li>• File/resource Access Failure :Change ownership</li> <li>• File/resource Access Success: Change property</li> <li>• File/resource Access Success: Change ownership</li> <li>• Solaris BSM: Audit policy changes</li> <li>• Solaris BSM: set, create, change passwords</li> <li>• Syslog: Password changed</li> </ul>	<ul style="list-style-type: none"> <li>• Agent not running</li> <li>• Audit log cleared</li> <li>• Directory permission change</li> <li>• Eventlog full</li> <li>• EventTracker cab integrity checksum failure</li> <li>• Excessive ping failures - system(s) are not reachable</li> <li>• Excessive file deletes on a computer</li> <li>• Excessive access failures on a specific computer</li> <li>• Excessive access failures in your enterprise</li> </ul>
System And Information Integrity	<p><b>SI-4 Information System Monitoring Tools and Techniques</b></p> <p><b>8500.2: EBBD-1, EBVC-1, ECID-1 DCID 6/3: 4.B.2.a(5)(b), 6.B.3.a(8)</b></p>	<p>Too many to list, including reports on Window, UNIX, Linux, network devices including firewalls (CISCO PIX, Checkpoint) routers and switches, infrastructure applications like Citrix, IIS, databases and many more...</p>	<ul style="list-style-type: none"> <li>• Excessive remote connections established on a local network port</li> <li>• Excessive logon failures in your enterprise</li> <li>• Excessive access failures in your enterprise</li> <li>• Excessive access failures on specific computer</li> <li>• Excessive file deletes on a computer</li> <li>• Excessive access failure by user</li> <li>• Logon Failures</li> <li>• Logon Failures from a specific computer</li> <li>• Excessive Logon failures due to bad password</li> <li>• Excessive remote connections established</li> <li>• Excessive User Lockout</li> <li>• ISA Server: Port Scan Detected</li> <li>• ISA Server: Land Attack detected</li> <li>• ISA Server: Out-of-bound attack</li> <li>• ISA Server: Ping attack</li> <li>• ISA Server: Spoof attack</li> </ul>

FISMA Requirement (NIST)		EventTracker	
Family	Control	Reports	Sample Alerts
			<ul style="list-style-type: none"> <li>• ISA Server: UDP attack</li> <li>• Netscreen: IDS Intrusion detected</li> <li>• Netscreen: Security device error</li> <li>• CISCO PIX: IDS Intrusion detected</li> </ul>
	<b>SI-7 Software and Information Integrity</b>  <b>8500.2: ECSD-2</b> <b>DCID 6/3: 4.B.1.c(2)(b)</b>	<ul style="list-style-type: none"> <li>• EventTracker: Service changes</li> <li>• Snort: Denial of service alerts</li> <li>• System: Service control manager</li> <li>• EventTracker: Software install/uninstall</li> <li>• Solaris BSM: Package management</li> </ul>	<ul style="list-style-type: none"> <li>• Detected Software install</li> </ul>