



Technology Area

DEFINITION

<i>Name</i>	System Life Cycle Security
<i>Description</i>	System Life Cycle Security is a method for addressing security in a system during its planning and continues through system acquisition and development, implementation, operations and maintenance and ends with the disposition of the system.
<i>Rationale</i>	Security vulnerabilities can occur during any phase of the system life cycle process. Addressing security in every phase gives an agency confidence that the system will function with a minimum of risk.
<i>Benefits</i>	<p>Integrating security into the systems development lifecycle is important for the following reasons:</p> <ul style="list-style-type: none"> • It is more effective. Meaningful security is easier to achieve when security issues are considered as a part of a routine development process, and security safeguards are integrated into the system during its design. • It is less expensive. To retrofit security is generally more expensive than to integrate it into an application. • It is less obtrusive. When security safeguards are integral to a system, they are usually easier to use.

ASSOCIATED ARCHITECTURE LEVELS

<i>List the Domain Name</i>	Security
<i>List the Discipline Name</i>	Management Controls

Associated Compliance Components

<i>List the Compliance Component Names</i>	<ul style="list-style-type: none"> • Initiation Phase • Acquisition and Development Phase • Implementation Phase • Operation and Maintenance Phase (Patch Management) • Disposal Phase
--	---

Associated Product Components

<i>List the Product Component Names</i>	<ul style="list-style-type: none"> • cyberCide (twilight) • DataEraser (twilight) • DataGone (twilight) • DBAN (sunset - CONFIDENTIAL) • Disk Wipe (twilight) • East-Tec Sanitizer (twilight) • Eraser (sunset - CONFIDENTIAL) • FDISK (sunset - CONFIDENTIAL) • GDisk (twilight) • KillIDisk (current) • Wipe Drive (current)
---	---

TECHNOLOGY AREA DETAIL

<i>Supporting Documentation</i>	Federal Information Processing Standards (FIPS) Publication (PUB) 73, Guidelines for Security of Computer Applications, June 1980; NIST SPEC PUB 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, April 1988; NIST SPEC PUB 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996
---------------------------------	--

<i>Document Source Reference #</i>	www.csrc.nist.gov/publications/nistpubs
------------------------------------	--

Standard Organization / Government Body

<i>Name</i>	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	<i>Website</i>	http://csrc.nist.gov/
-------------	---	----------------	---

<i>Contact Information</i>	inquiries@nist.gov
----------------------------	--

<i>Name</i>		<i>Website</i>	
-------------	--	----------------	--

<i>Contact Information</i>	
----------------------------	--

KEYWORDS

<i>List Keywords</i>	System Life Cycle, exploitation, bugs, vulnerabilities, malicious, remediation, maintenance, monitor, holes, defects, bad code, management, procedures, planning, sensitive, data, evaluate, test, inspect, certification, accreditation, requirements, incorporate, SDLC, risk, threat, controls, policy, architecture, laws, regulations, agreements, assurance, cost, estimates, integrate, impact, environment, schedule, performance, baseline.
----------------------	--

CURRENT STATUS

<i>Provide the Current Status</i>	<input type="checkbox"/> <i>In Development</i> <input type="checkbox"/> <i>Under Review</i> <input checked="" type="checkbox"/> <i>Approved</i> <input type="checkbox"/> <i>Rejected</i>
-----------------------------------	--

AUDIT TRAIL

<i>Creation Date</i>	09/07/06	<i>Date Accepted / Rejected</i>	9/12/06
<i>Reason for Rejection</i>			
<i>Last Date Reviewed</i>		<i>Last Date Updated</i>	
<i>Reason for Update</i>			