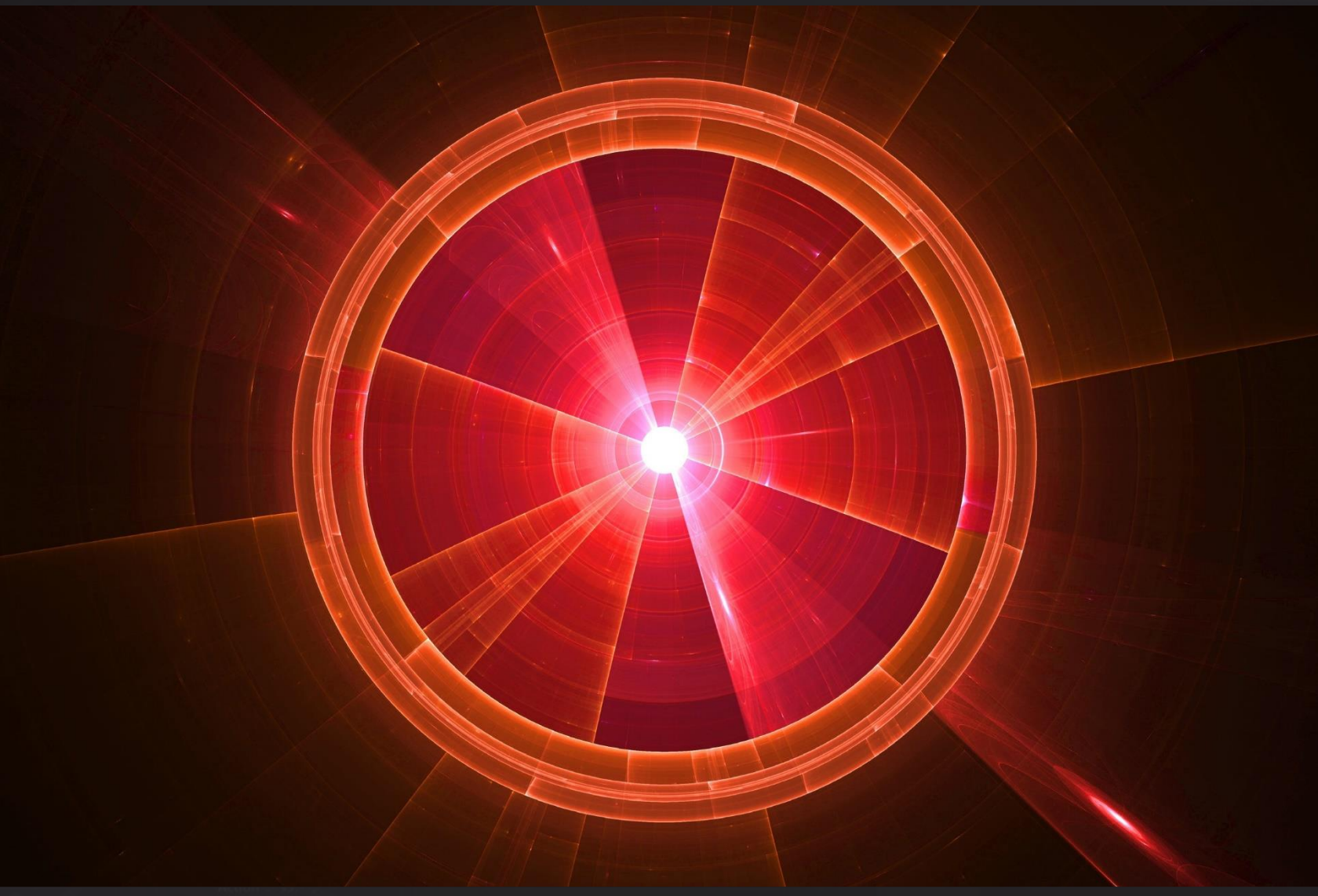
GRAMMATECH

DEFENSE INFORMATION SYSTEMS AGENCY(DISA) APPLICATION SECURITY AND DEVELOPMENT SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) FINDING IDS

MAPPED TO CODESONAR® 7.2 WARNING CLASSES



TRUSTED LEADERS OF SOFTWARE ASSURANCE AND ADVANCED CYBER-SECURITY SOLUTIONS

WWW.GRAMMATECH.COM

INTRODUCTION

CodeSonar supports checking for violations of some of the requirements laid out in the DISA Application Security and Development STIG.

In particular, CodeSonar 7.2 provides mappings between CodeSonar warning classes and Finding IDs for two versions of this STIG: Version 4 Release 3 (release date April 28, 2017) and Version3 Release 10 (release date January 23, 2015).

Every CodeSonar warning report includes any Finding IDs from these versions that are closely mapped to the warning's class. (The close mapping for a warning class is the set of categories—including Application Security and Development Security STIG Finding IDs—that most closely match the class, if any).

You can configure CodeSonar to enable and disable warning classes mapped to specific Finding IDs from either or both of these versions, or use build presets to enable all warning classes that are closely mapped to any Finding ID from one or both versions. In addition, you can use the CodeSonar search function to find warnings related to specific Finding IDs, or to any Finding ID from one or both versions.

We also provide broad mappings for these two STIG versions. The broad mapping for Application Security and Development Security STIG and a given warning class includes the close mapping forthe class, plus any other Application Security and Development Security STIG finding IDs that are related to the class in a meaningful way, but not eligible for the close mapping.

This document contains four tables showing mappings between CodeSonar v7.2 warning classes and Finding IDs from the Application Security and Development Security STIG.

- Mappings for the DISA Application Security and Development Security STIG version 4release 3 (v4r3).
  - Close DISA Application Security and Development STIG v4r3 Mappings(CodeSonar v7.2)
  - Broad DISA Application Security and Development STIG v4r3 Mappings(CodeSonar v7.2)
- Mappings for the DISA Application Security and Development Security STIG version 3release 10 (v3r10).
  - Close DISA Application Security and Development STIG v3r10 Mappings(CodeSonar v7.2)
  - Broad DISA Application Security and Development STIG v3r10 mappings(CodeSonar v7.2)

For more information on the DISA Application Security and Development Security

STIG:https://iase.disa.mil/stigs/app-security/app-security/Pages/app-security.aspx

GrammaTech is a leading global provider of application testing (AST) solutions used by the world's most security conscious organizations to detect, measure, analyze and resolve vulnerabilities for software they develop or use. The company is also a trusted cybersecurity and artificial intelligence research partner for the nation's civil, defense, and intelligence agencies.

CLOSE DISA APPLICATION SECURITY AND DEVELOPMENT STIG V4R3 MAPPINGS (CODESONAR V7.2)

The following table contains CodeSonar warning classes that are closely mapped to Finding IDs from version 4, release 3 of the DISA Application Security and Development Security STIG weakness IDs.

Rule	Rule Name	Supported
DISA-4r3:V-69239	The application must provide a capability to limit the number of logon sessions per user.	No
DISA-4r3:V-69241	The application must clear temporary storage and cookies when the session is terminated.	No
DISA-4r3:V-69243	The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	No
DISA-4r3:V-69245	The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	No
DISA-4r3:V-69247	Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	No
DISA-4r3:V-69249	The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	No
DISA-4r3:V-69251	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	No
DISA-4r3:V-69253	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	No
DISA-4r3:V-69255	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	No
DISA-4r3:V-69257	The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	Yes
DISA-4r3:V-69259	The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	Yes
DISA-4r3:V-69261	Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	No
DISA-4r3:V-69279	Messages protected with WS_Security must use time stamps with creation and expiration times.	No
DISA-4r3:V-69281	Validity periods must be verified on all application messages using WS-Security or SAML assertions.	No
DISA-4r3:V-69283	The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	No
DISA-4r3:V-69285	The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	No
DISA-4r3:V-69287	The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	No
DISA-4r3:V-69289	The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	No
DISA-4r3:V-69291	The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	No
DISA-4r3:V-69293	The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	No
DISA-4r3:V-69295	The application must provide automated mechanisms for supporting account management functions.	No
DISA-4r3:V-69297	Shared/group account credentials must be terminated when members leave the group.	No
DISA-4r3:V-69299	The application must automatically remove or disable temporary user accounts 72 hours after account creation.	No
DISA-4r3:V-69301	The application must automatically disable accounts after a 35 day period of account inactivity.	No
DISA-4r3:V-69303	Unnecessary application accounts must be disabled, or deleted.	No

DISA-4r3:V-69305	The application must automatically audit account creation.	No
DISA-4r3:V-69307	The application must automatically audit account modification.	No
DISA-4r3:V-69309	The application must automatically audit account disabling actions.	No
DISA-4r3:V-69311	The application must automatically audit account removal actions.	No
DISA-4r3:V-69313	The application must notify System Administrators and Information System Security Officers when accounts are created.	No
DISA-4r3:V-69315	The application must notify System Administrators and Information System Security Officers when accounts are modified.	No
DISA-4r3:V-69317	The application must notify System Administrators and Information System Security Officers of account disabling actions.	No
DISA-4r3:V-69319	The application must notify System Administrators and Information System Security Officers of account removal actions.	No
DISA-4r3:V-69321	The application must automatically audit account enabling actions.	No
DISA-4r3:V-69323	The application must notify System Administrators and Information System Security Officers of account enabling actions.	No
DISA-4r3:V-69325	Application data protection requirements must be identified and documented.	No
DISA-4r3:V-69327	The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	No
DISA-4r3:V-69329	The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	No
DISA-4r3:V-69331	The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	No
DISA-4r3:V-69333	The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	No
DISA-4r3:V-69335	The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	No
DISA-4r3:V-69337	The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	No
DISA-4r3:V-69339	The application must execute without excessive account permissions.	No
DISA-4r3:V-69341	The application must audit the execution of privileged functions.	No
DISA-4r3:V-69343	The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	No
DISA-4r3:V-69347	The application administrator must follow an approved process to unlock locked user accounts.	No
DISA-4r3:V-69349	The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	No
DISA-4r3:V-69351	The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	No
DISA-4r3:V-69353	The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	No
DISA-4r3:V-69355	The application must display the time and date of the users last successful logon.	No
DISA-4r3:V-69357	The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	No
DISA-4r3:V-69359	For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.	No
DISA-4r3:V-69361	The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	No
DISA-4r3:V-69363	The application must provide audit record generation capability for the creation of session IDs.	No
DISA-4r3:V-69365	The application must provide audit record generation capability for the destruction of session IDs.	No
DISA-4r3:V-69367	The application must provide audit record generation capability for the renewal of session IDs.	No
DISA-4r3:V-69369	The application must not write sensitive data into the application logs.	No

DISA-4r3:V-69371	The application must provide audit record generation capability for session timeouts.	No
DISA-4r3:V-69373	The application must record a time stamp indicating when the event occurred.	No
DISA-4r3:V-69375	The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	No
DISA-4r3:V-69377	The application must provide audit record generation capability for connecting system IP addresses.	No
DISA-4r3:V-69379	The application must record the username or user ID of the user associated with the event.	No
DISA-4r3:V-69381	The application must generate audit records when successful/unsuccessful attempts to access privileges occur.	No
DISA-4r3:V-69383	The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	No
DISA-4r3:V-69385	The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	No
DISA-4r3:V-69387	The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69389	The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	No
DISA-4r3:V-69391	The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	No
DISA-4r3:V-69393	The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	No
DISA-4r3:V-69395	The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69397	The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	No
DISA-4r3:V-69399	The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	No
DISA-4r3:V-69401	The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	No
DISA-4r3:V-69403	The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69405	The application must generate audit records when successful/unsuccessful logon attempts occur.	No
DISA-4r3:V-69407	The application must generate audit records for privileged activities or other system-level access.	No
DISA-4r3:V-69409	The application must generate audit records showing starting and ending time for user access to the system.	No
DISA-4r3:V-69411	The application must generate audit records when successful/unsuccessful accesses to objects occur.	No
DISA-4r3:V-69413	The application must generate audit records for all direct access to the information system.	No
DISA-4r3:V-69415	The application must generate audit records for all account creations, modifications, disabling, and termination events.	No
DISA-4r3:V-69417	The application must provide the capability for authorized users to select a user session to capture/record or view/hear.	No
DISA-4r3:V-69419	The application must initiate session auditing upon startup.	No
DISA-4r3:V-69421	The application must log application shutdown events.	No
DISA-4r3:V-69423	The application must log destination IP addresses.	No
DISA-4r3:V-69425	The application must log user actions involving access to data.	No
DISA-4r3:V-69427	The application must log user actions involving changes to data.	No
DISA-4r3:V-69429	The application must produce audit records containing information to establish when (date and time) the events occurred.	No
DISA-4r3:V-69431	The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	No
DISA-4r3:V-69433	When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	No
DISA-4r3:V-69435	The application must produce audit records that contain information to establish the outcome of the events.	No

DISA-4r3:V-69437	The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	No
DISA-4r3:V-69439	The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	No
DISA-4r3:V-69441	The application must implement transaction recovery logs when transaction based.	No
DISA-4r3:V-69443	The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	No
DISA-4r3:V-69445	The application must off-load audit records onto a different system or media than the system being audited.	No
DISA-4r3:V-69447	The application must be configured to write application logs to a centralized log repository.	No
DISA-4r3:V-69449	The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	No
DISA-4r3:V-69451	Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	No
DISA-4r3:V-69453	The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	No
DISA-4r3:V-69455	The application must shut down by default upon audit failure (unless availability is an overriding concern).	No
DISA-4r3:V-69457	The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	No
DISA-4r3:V-69459	The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	No
DISA-4r3:V-69461	The application must provide an audit reduction capability that supports on-demand reporting requirements.	No
DISA-4r3:V-69463	The application must provide an audit reduction capability that supports on-demand audit review and analysis.	No
DISA-4r3:V-69465	The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	No
DISA-4r3:V-69467	The application must provide a report generation capability that supports on-demand audit review and analysis.	No
DISA-4r3:V-69469	The application must provide a report generation capability that supports on-demand reporting requirements.	No
DISA-4r3:V-69471	The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	No
DISA-4r3:V-69473	The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	No
DISA-4r3:V-69475	The application must provide a report generation capability that does not alter original content or time ordering of audit records.	No
DISA-4r3:V-69477	The applications must use internal system clocks to generate time stamps for audit records.	No
DISA-4r3:V-69479	The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	No
DISA-4r3:V-69481	The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.	No
DISA-4r3:V-69483	The application must protect audit information from any type of unauthorized read access.	No
DISA-4r3:V-69485	The application must protect audit information from unauthorized modification.	No
DISA-4r3:V-69487	The application must protect audit information from unauthorized deletion.	No
DISA-4r3:V-69489	The application must protect audit tools from unauthorized access.	No
DISA-4r3:V-69491	The application must protect audit tools from unauthorized modification.	No
DISA-4r3:V-69493	The application must protect audit tools from unauthorized deletion.	No
DISA-4r3:V-69495	The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	No
DISA-4r3:V-69497	The application must use cryptographic mechanisms to protect the integrity of audit information.	No
DISA-4r3:V-69499	Application audit tools must be cryptographically hashed.	No

DISA-4r3:V-69501	The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	No
DISA-4r3:V-69503	The application must prohibit user installation of software without explicit privileged status.	No
DISA-4r3:V-69505	The application must enforce access restrictions associated with changes to application configuration.	No
DISA-4r3:V-69507	The application must audit who makes configuration changes to the application.	No
DISA-4r3:V-69509	The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.	No
DISA-4r3:V-69511	The applications must limit privileges to change the software resident within software libraries.	No
DISA-4r3:V-69513	An application vulnerability assessment must be conducted.	No
DISA-4r3:V-69515	The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	No
DISA-4r3:V-69517	The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	No
DISA-4r3:V-69519	The application must be configured to disable non-essential capabilities.	No
DISA-4r3:V-69521	The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	No
DISA-4r3:V-69523	The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	No
DISA-4r3:V-69525	The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	No
DISA-4r3:V-69527	The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	No
DISA-4r3:V-69529	The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	No
DISA-4r3:V-69531	The application must accept Personal Identity Verification (PIV) credentials.	No
DISA-4r3:V-69533	The application must electronically verify Personal Identity Verification (PIV) credentials.	No
DISA-4r3:V-69535	The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	No
DISA-4r3:V-69537	The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	No
DISA-4r3:V-69539	The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	No
DISA-4r3:V-69541	The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	No
DISA-4r3:V-69543	The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	No
DISA-4r3:V-69545	The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	No
DISA-4r3:V-69547	The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	No
DISA-4r3:V-69549	The application must authenticate all network connected endpoint devices before establishing any connection.	No
DISA-4r3:V-69551	Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	No
DISA-4r3:V-69553	The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	No
DISA-4r3:V-69555	The application must enforce a minimum 15-character password length.	No
DISA-4r3:V-69557	The application must enforce password complexity by requiring that at least one upper-case character be used.	No
DISA-4r3:V-69559	The application must enforce password complexity by requiring that at least one lower-case character be used.	No

DISA-4r3:V-69561	The application must enforce password complexity by requiring that at least one numeric character be used.	No
DISA-4r3:V-69563	The application must enforce password complexity by requiring that at least one special character be used.	No
DISA-4r3:V-69565	The application must require the change of at least 8 of the total number of characters when passwords are changed.	No
DISA-4r3:V-69567	The application must only store cryptographic representations of passwords.	Yes
DISA-4r3:V-69569	The application must transmit only cryptographically-protected passwords.	Yes
DISA-4r3:V-69571	The application must enforce 24 hours/1 day as the minimum password lifetime.	No
DISA-4r3:V-69573	The application must enforce a 60-day maximum password lifetime restriction.	No
DISA-4r3:V-69575	The application must prohibit password reuse for a minimum of five generations.	No
DISA-4r3:V-69577	The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	No
DISA-4r3:V-70145	The application password must not be changeable by users other than the administrator or the user with which the password is associated.	No
DISA-4r3:V-70147	The application must terminate existing user sessions upon account deletion.	No
DISA-4r3:V-70149	The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	No
DISA-4r3:V-70151	The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	No
DISA-4r3:V-70153	The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	No
DISA-4r3:V-70155	The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	No
DISA-4r3:V-70157	The application must not display passwords/PINs as clear text.	No
DISA-4r3:V-70159	The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	No
DISA-4r3:V-70161	The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	No
DISA-4r3:V-70163	The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	No
DISA-4r3:V-70165	The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	No
DISA-4r3:V-70167	The application must accept FICAM-approved third-party credentials.	No
DISA-4r3:V-70169	The application must conform to FICAM-issued profiles.	No
DISA-4r3:V-70171	Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	No
DISA-4r3:V-70173	The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	No
DISA-4r3:V-70175	Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	No
DISA-4r3:V-70177	Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	No
DISA-4r3:V-70179	Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	No
DISA-4r3:V-70181	The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	No
DISA-4r3:V-70183	The application must terminate all sessions and network connections when non-local maintenance is completed.	No
DISA-4r3:V-70185	The application must not be vulnerable to race conditions.	Yes
DISA-4r3:V-70187	The application must terminate all network connections associated with a communications session at the end of the session.	No

DISA-4r3:V-70189	The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	No
DISA-4r3:V-70191	The application must utilize FIPS-validated cryptographic modules when signing application components.	Yes
DISA-4r3:V-70193	The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	Yes
DISA-4r3:V-70195	The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	Yes
DISA-4r3:V-70197	Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	No
DISA-4r3:V-70199	The application user interface must be either physically or logically separated from data storage and management interfaces.	No
DISA-4r3:V-70201	The application must set the HTTPOnly flag on session cookies.	No
DISA-4r3:V-70203	The application must set the secure flag on session cookies.	No
DISA-4r3:V-70205	The application must not expose session IDs.	No
DISA-4r3:V-70207	The application must destroy the session ID value and/or cookie on logoff or browser close.	No
DISA-4r3:V-70209	Applications must use system-generated session identifiers that protect against session fixation.	No
DISA-4r3:V-70211	Applications must validate session identifiers.	No
DISA-4r3:V-70213	Applications must not use URL embedded session IDs.	No
DISA-4r3:V-70215	The application must not re-use or recycle session IDs.	No
DISA-4r3:V-70217	The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	Yes
DISA-4r3:V-70219	The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	No
DISA-4r3:V-70221	The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	No
DISA-4r3:V-70223	In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	No
DISA-4r3:V-70225	The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.	No
DISA-4r3:V-70227	The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	No
DISA-4r3:V-70229	The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	Yes
DISA-4r3:V-70231	The application must isolate security functions from non-security functions.	No
DISA-4r3:V-70233	The application must maintain a separate execution domain for each executing process.	No
DISA-4r3:V-70235	Applications must prevent unauthorized and unintended information transfer via shared system resources.	No
DISA-4r3:V-70237	XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	No
DISA-4r3:V-70239	The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	No
DISA-4r3:V-70241	The web service design must include redundancy mechanisms when used with high-availability systems.	No
DISA-4r3:V-70243	An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	No
DISA-4r3:V-70245	The application must protect the confidentiality and integrity of transmitted information.	Yes
DISA-4r3:V-70247	The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).	No
DISA-4r3:V-70249	The application must maintain the confidentiality and integrity of information during preparation for transmission.	No

DISA-4r3:V-70251	The application must maintain the confidentiality and integrity of information during reception.	No
DISA-4r3:V-70253	The application must not disclose unnecessary information to users.	No
DISA-4r3:V-70255	The application must not store sensitive information in hidden fields.	No
DISA-4r3:V-70257	The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	Yes
DISA-4r3:V-70259	The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	No
DISA-4r3:V-70261	The application must protect from command injection.	Yes
DISA-4r3:V-70263	The application must protect from canonical representation vulnerabilities.	No
DISA-4r3:V-70265	The application must validate all input.	Yes
DISA-4r3:V-70267	The application must not be vulnerable to SQL Injection.	Yes
DISA-4r3:V-70269	The application must not be vulnerable to XML-oriented attacks.	Yes
DISA-4r3:V-70271	The application must not be subject to input handling vulnerabilities.	Yes
DISA-4r3:V-70273	The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	No
DISA-4r3:V-70275	The application must reveal error messages only to the ISSO, ISSM, or SA.	No
DISA-4r3:V-70277	The application must not be vulnerable to overflow attacks.	Yes
DISA-4r3:V-70279	The application must remove organization-defined software components after updated versions have been installed.	No
DISA-4r3:V-70281	Security-relevant software updates and patches must be kept up to date.	No
DISA-4r3:V-70283	The application performing organization-defined security functions must verify correct operation of security functions.	No
DISA-4r3:V-70285	The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	No
DISA-4r3:V-70287	The application must notify the ISSO and ISSM of failed security verification tests.	No
DISA-4r3:V-70289	Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	No
DISA-4r3:V-70291	The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	No
DISA-4r3:V-70293	Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	No
DISA-4r3:V-70295	The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	No
DISA-4r3:V-70297	The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	No
DISA-4r3:V-70301	The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	No
DISA-4r3:V-70303	The ISSO must ensure active vulnerability testing is performed.	No
DISA-4r3:V-70305	AO risk acceptance must be obtained for all public domain, shareware, freeware, and other software products/libraries with both (1) no source code to review, repair, and extend, and (2) limited or no warranty, when such products are required for mission accomplishment.	No
DISA-4r3:V-70307	Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	No
DISA-4r3:V-70309	The designer must ensure the application does not store configuration and control files in the same directory as user data.	No
DISA-4r3:V-70311	The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by following available guidance.	No
DISA-4r3:V-70313	New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPSM).	No
DISA-4r3:V-70317	The application must be registered with the DoD Ports and Protocols Database.	No
DISA-4r3:V-70339	The Configuration Management (CM) repository must be properly patched and STIG compliant.	No
DISA-4r3:V-70341	Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	No

DISA-4r3:V-70343	A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	No
DISA-4r3:V-70345	A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	No
DISA-4r3:V-70347	The application services and interfaces must be compatible with and ready for IPv6 networks.	No
DISA-4r3:V-70349	The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	No
DISA-4r3:V-70351	A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	No
DISA-4r3:V-70353	Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	No
DISA-4r3:V-70355	Data backup must be performed at required intervals in accordance with DoD policy.	No
DISA-4r3:V-70357	Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	No
DISA-4r3:V-70359	Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	No
DISA-4r3:V-70361	The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	No
DISA-4r3:V-70363	The application must not contain embedded authentication data.	Yes
DISA-4r3:V-70365	The application must have the capability to mark sensitive/classified output when required.	No
DISA-4r3:V-70367	Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	No
DISA-4r3:V-70369	Application files must be cryptographically hashed prior to deploying to DoD operational networks.	No
DISA-4r3:V-70371	At least one tester must be designated to test for security flaws in addition to functional testing.	No
DISA-4r3:V-70373	Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	No
DISA-4r3:V-70375	An application code review must be performed on the application.	No
DISA-4r3:V-70377	Code coverage statistics must be maintained for each release of the application.	No
DISA-4r3:V-70379	Flaws found during a code review must be tracked in a defect tracking system.	No
DISA-4r3:V-70381	The changes to the application must be assessed for IA and accreditation impact prior to implementation.	No
DISA-4r3:V-70383	Security flaws must be fixed or addressed in the project plan.	No
DISA-4r3:V-70385	The application development team must follow a set of coding standards.	No
DISA-4r3:V-70387	The designer must create and update the Design Document for each release of the application.	No
DISA-4r3:V-70389	Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	No
DISA-4r3:V-70391	The application must not be subject to error handling vulnerabilities.	Yes
DISA-4r3:V-70393	The application development team must provide an application incident response plan.	No
DISA-4r3:V-70395	All products must be supported by the vendor or the development team.	No
DISA-4r3:V-70397	The application must be decommissioned when maintenance or support is no longer available.	No
DISA-4r3:V-70399	Procedures must be in place to notify users when an application is decommissioned.	No
DISA-4r3:V-70401	Unnecessary built-in application accounts must be disabled.	No
DISA-4r3:V-70403	Default passwords must be changed.	No
DISA-4r3:V-70405	An Application Configuration Guide must be created and included with the application.	No
DISA-4r3:V-70407	If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	No
DISA-4r3:V-70409	The designer must ensure uncategorized or emerging mobile code is not used in applications.	No
DISA-4r3:V-70411	Production database exports must have database administration credentials and sensitive data removed before releasing the export.	No
DISA-4r3:V-70413	Protections against DoS attacks must be implemented.	No
DISA-4r3:V-70415	The system must alert an administrator when low resource conditions are encountered.	No

DISA-4r3:V-70417	At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	No
DISA-4r3:V-70419	The application must provide notifications or alerts when product update and security related patches are available.	No
DISA-4r3:V-70421	Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	No
DISA-4r3:V-70423	The application must generate audit records when concurrent logons from different workstations occur.	No
DISA-4r3:V-70425	The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	No

BROAD DISA APPLICATION SECURITY AND DEVELOPMENT STIG V4R3 MAPPINGS (CODESONAR V7.2)

The following table contains CodeSonar warning classes that are broadly mapped to Finding IDs from version 4, release 3 of the DISA Application Security and Development Security STIG.

Rule	Rule Name	Supported
DISA-4r3:V-69239	The application must provide a capability to limit the number of logon sessions per user.	No
DISA-4r3:V-69241	The application must clear temporary storage and cookies when the session is terminated.	No
DISA-4r3:V-69243	The application must automatically terminate the non-privileged user session and log off non-privileged users after a 15 minute idle time period has elapsed.	No
DISA-4r3:V-69245	The application must automatically terminate the admin user session and log off admin users after a 10 minute idle time period is exceeded.	No
DISA-4r3:V-69247	Applications requiring user access authentication must provide a logoff capability for user initiated communication session.	No
DISA-4r3:V-69249	The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions.	No
DISA-4r3:V-69251	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in storage.	No
DISA-4r3:V-69253	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in process.	No
DISA-4r3:V-69255	The application must associate organization-defined types of security attributes having organization-defined security attribute values with information in transmission.	No
DISA-4r3:V-69257	The application must implement DoD-approved encryption to protect the confidentiality of remote access sessions.	Yes
DISA-4r3:V-69259	The application must implement cryptographic mechanisms to protect the integrity of remote access sessions.	Yes
DISA-4r3:V-69261	Applications with SOAP messages requiring integrity must include the following message elements:-Message ID-Service Request-Timestamp-SAML Assertion (optionally included in messages) and all elements of the message must be digitally signed.	No
DISA-4r3:V-69279	Messages protected with WS_Security must use time stamps with creation and expiration times.	No
DISA-4r3:V-69281	Validity periods must be verified on all application messages using WS-Security or SAML assertions.	No
DISA-4r3:V-69283	The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	No
DISA-4r3:V-69285	The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary.	No
DISA-4r3:V-69287	The application must use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	No
DISA-4r3:V-69289	The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion.	No
DISA-4r3:V-69291	The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion.	No
DISA-4r3:V-69293	The application must ensure messages are encrypted when the SessionIndex is tied to privacy data.	No
DISA-4r3:V-69295	The application must provide automated mechanisms for supporting account management functions.	No
DISA-4r3:V-69297	Shared/group account credentials must be terminated when members leave the group.	No
DISA-4r3:V-69299	The application must automatically remove or disable temporary user accounts 72 hours after account creation.	No
DISA-4r3:V-69301	The application must automatically disable accounts after a 35 day period of account inactivity.	No
DISA-4r3:V-69303	Unnecessary application accounts must be disabled, or deleted.	No
DISA-4r3:V-69305	The application must automatically audit account creation.	No
DISA-4r3:V-69307	The application must automatically audit account modification.	No

DISA-4r3:V-69309	The application must automatically audit account disabling actions.	No
DISA-4r3:V-69311	The application must automatically audit account removal actions.	No
DISA-4r3:V-69313	The application must notify System Administrators and Information System Security Officers when accounts are created.	No
DISA-4r3:V-69315	The application must notify System Administrators and Information System Security Officers when accounts are modified.	No
DISA-4r3:V-69317	The application must notify System Administrators and Information System Security Officers of account disabling actions.	No
DISA-4r3:V-69319	The application must notify System Administrators and Information System Security Officers of account removal actions.	No
DISA-4r3:V-69321	The application must automatically audit account enabling actions.	No
DISA-4r3:V-69323	The application must notify System Administrators and Information System Security Officers of account enabling actions.	No
DISA-4r3:V-69325	Application data protection requirements must be identified and documented.	No
DISA-4r3:V-69327	The application must utilize organization-defined data mining detection techniques for organization-defined data storage objects to adequately detect data mining attempts.	No
DISA-4r3:V-69329	The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	No
DISA-4r3:V-69331	The application must enforce organization-defined discretionary access control policies over defined subjects and objects.	No
DISA-4r3:V-69333	The application must enforce approved authorizations for controlling the flow of information within the system based on organization-defined information flow control policies.	No
DISA-4r3:V-69335	The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on organization-defined information flow control policies.	No
DISA-4r3:V-69337	The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	No
DISA-4r3:V-69339	The application must execute without excessive account permissions.	No
DISA-4r3:V-69341	The application must audit the execution of privileged functions.	No
DISA-4r3:V-69343	The application must enforce the limit of three consecutive invalid logon attempts by a user during a 15 minute time period.	No
DISA-4r3:V-69347	The application administrator must follow an approved process to unlock locked user accounts.	No
DISA-4r3:V-69349	The application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	No
DISA-4r3:V-69351	The application must retain the Standard Mandatory DoD Notice and Consent Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access.	No
DISA-4r3:V-69353	The publicly accessible application must display the Standard Mandatory DoD Notice and Consent Banner before granting access to the application.	No
DISA-4r3:V-69355	The application must display the time and date of the users last successful logon.	No
DISA-4r3:V-69357	The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.	No
DISA-4r3:V-69359	For applications providing audit record aggregation, the application must compile audit records from organization-defined information system components into a system-wide audit trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the audit trail.	No
DISA-4r3:V-69361	The application must provide the capability for organization-identified individuals or roles to change the auditing to be performed on all application components, based on all selectable event criteria within organization-defined time thresholds.	No
DISA-4r3:V-69363	The application must provide audit record generation capability for the creation of session IDs.	No
DISA-4r3:V-69365	The application must provide audit record generation capability for the destruction of session IDs.	No
DISA-4r3:V-69367	The application must provide audit record generation capability for the renewal of session IDs.	No
DISA-4r3:V-69369	The application must not write sensitive data into the application logs.	No
DISA-4r3:V-69371	The application must provide audit record generation capability for session timeouts.	No
DISA-4r3:V-69373	The application must record a time stamp indicating when the event occurred.	No

DISA-4r3:V-69375	The application must provide audit record generation capability for HTTP headers including User-Agent, Referer, GET, and POST.	No
DISA-4r3:V-69377	The application must provide audit record generation capability for connecting system IP addresses.	No
DISA-4r3:V-69379	The application must record the username or user ID of the user associated with the event.	No
DISA-4r3:V-69381	The application must generate audit records when successful/unsuccessful attempts to access privileges occur.	No
DISA-4r3:V-69383	The application must generate audit records when successful/unsuccessful attempts to access security objects occur.	No
DISA-4r3:V-69385	The application must generate audit records when successful/unsuccessful attempts to access security levels occur.	No
DISA-4r3:V-69387	The application must generate audit records when successful/unsuccessful attempts to access categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69389	The application must generate audit records when successful/unsuccessful attempts to modify privileges occur.	No
DISA-4r3:V-69391	The application must generate audit records when successful/unsuccessful attempts to modify security objects occur.	No
DISA-4r3:V-69393	The application must generate audit records when successful/unsuccessful attempts to modify security levels occur.	No
DISA-4r3:V-69395	The application must generate audit records when successful/unsuccessful attempts to modify categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69397	The application must generate audit records when successful/unsuccessful attempts to delete privileges occur.	No
DISA-4r3:V-69399	The application must generate audit records when successful/unsuccessful attempts to delete security levels occur.	No
DISA-4r3:V-69401	The application must generate audit records when successful/unsuccessful attempts to delete application database security objects occur.	No
DISA-4r3:V-69403	The application must generate audit records when successful/unsuccessful attempts to delete categories of information (e.g., classification levels) occur.	No
DISA-4r3:V-69405	The application must generate audit records when successful/unsuccessful logon attempts occur.	No
DISA-4r3:V-69407	The application must generate audit records for privileged activities or other system-level access.	No
DISA-4r3:V-69409	The application must generate audit records showing starting and ending time for user access to the system.	No
DISA-4r3:V-69411	The application must generate audit records when successful/unsuccessful accesses to objects occur.	No
DISA-4r3:V-69413	The application must generate audit records for all direct access to the information system.	No
DISA-4r3:V-69415	The application must generate audit records for all account creations, modifications, disabling, and termination events.	No
DISA-4r3:V-69417	The application must provide the capability for authorized users to select a user session to capture/record or view/hear.	No
DISA-4r3:V-69419	The application must initiate session auditing upon startup.	No
DISA-4r3:V-69421	The application must log application shutdown events.	No
DISA-4r3:V-69423	The application must log destination IP addresses.	No
DISA-4r3:V-69425	The application must log user actions involving access to data.	No
DISA-4r3:V-69427	The application must log user actions involving changes to data.	No
DISA-4r3:V-69429	The application must produce audit records containing information to establish when (date and time) the events occurred.	No
DISA-4r3:V-69431	The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event.	No
DISA-4r3:V-69433	When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs.	No
DISA-4r3:V-69435	The application must produce audit records that contain information to establish the outcome of the events.	No
DISA-4r3:V-69437	The application must generate audit records containing information that establishes the identity of any individual or process associated with the event.	No

DISA-4r3:V-69439	The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users.	No
DISA-4r3:V-69441	The application must implement transaction recovery logs when transaction based.	No
DISA-4r3:V-69443	The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components.	No
DISA-4r3:V-69445	The application must off-load audit records onto a different system or media than the system being audited.	No
DISA-4r3:V-69447	The application must be configured to write application logs to a centralized log repository.	No
DISA-4r3:V-69449	The application must provide an immediate warning to the SA and ISSO (at a minimum) when allocated audit record storage volume reaches 75% of repository maximum audit record storage capacity.	No
DISA-4r3:V-69451	Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and ISSO (at a minimum) for all audit failure events.	No
DISA-4r3:V-69453	The application must alert the ISSO and SA (at a minimum) in the event of an audit processing failure.	No
DISA-4r3:V-69455	The application must shut down by default upon audit failure (unless availability is an overriding concern).	No
DISA-4r3:V-69457	The application must provide the capability to centrally review and analyze audit records from multiple components within the system.	No
DISA-4r3:V-69459	The application must provide the capability to filter audit records for events of interest based upon organization-defined criteria.	No
DISA-4r3:V-69461	The application must provide an audit reduction capability that supports on-demand reporting requirements.	No
DISA-4r3:V-69463	The application must provide an audit reduction capability that supports on-demand audit review and analysis.	No
DISA-4r3:V-69465	The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents.	No
DISA-4r3:V-69467	The application must provide a report generation capability that supports on-demand audit review and analysis.	No
DISA-4r3:V-69469	The application must provide a report generation capability that supports on-demand reporting requirements.	No
DISA-4r3:V-69471	The application must provide a report generation capability that supports after-the-fact investigations of security incidents.	No
DISA-4r3:V-69473	The application must provide an audit reduction capability that does not alter original content or time ordering of audit records.	No
DISA-4r3:V-69475	The application must provide a report generation capability that does not alter original content or time ordering of audit records.	No
DISA-4r3:V-69477	The applications must use internal system clocks to generate time stamps for audit records.	No
DISA-4r3:V-69479	The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	No
DISA-4r3:V-69481	The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision.	No
DISA-4r3:V-69483	The application must protect audit information from any type of unauthorized read access.	No
DISA-4r3:V-69485	The application must protect audit information from unauthorized modification.	No
DISA-4r3:V-69487	The application must protect audit information from unauthorized deletion.	No
DISA-4r3:V-69489	The application must protect audit tools from unauthorized access.	No
DISA-4r3:V-69491	The application must protect audit tools from unauthorized modification.	No
DISA-4r3:V-69493	The application must protect audit tools from unauthorized deletion.	No
DISA-4r3:V-69495	The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited.	No
DISA-4r3:V-69497	The application must use cryptographic mechanisms to protect the integrity of audit information.	No
DISA-4r3:V-69499	Application audit tools must be cryptographically hashed.	No
DISA-4r3:V-69501	The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value.	No
DISA-4r3:V-69503	The application must prohibit user installation of software without explicit privileged status.	No

DISA-4r3:V-69505	The application must enforce access restrictions associated with changes to application configuration.	No
DISA-4r3:V-69507	The application must audit who makes configuration changes to the application.	No
DISA-4r3:V-69509	The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the organization.	No
DISA-4r3:V-69511	The applications must limit privileges to change the software resident within software libraries.	No
DISA-4r3:V-69513	An application vulnerability assessment must be conducted.	No
DISA-4r3:V-69515	The application must prevent program execution in accordance with organization-defined policies regarding software program usage and restrictions, and/or rules authorizing the terms and conditions of software program usage.	No
DISA-4r3:V-69517	The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs.	No
DISA-4r3:V-69519	The application must be configured to disable non-essential capabilities.	No
DISA-4r3:V-69521	The application must be configured to use only functions, ports, and protocols permitted to it in the PPSM CAL.	No
DISA-4r3:V-69523	The application must require users to reauthenticate when organization-defined circumstances or situations require reauthentication.	No
DISA-4r3:V-69525	The application must require devices to reauthenticate when organization-defined circumstances or situations requiring reauthentication.	No
DISA-4r3:V-69527	The application must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).	No
DISA-4r3:V-69529	The application must use multifactor (Alt. Token) authentication for network access to privileged accounts.	No
DISA-4r3:V-69531	The application must accept Personal Identity Verification (PIV) credentials.	No
DISA-4r3:V-69533	The application must electronically verify Personal Identity Verification (PIV) credentials.	No
DISA-4r3:V-69535	The application must use multifactor (e.g., CAC, Alt. Token) authentication for network access to non-privileged accounts.	No
DISA-4r3:V-69537	The application must use multifactor (Alt. Token) authentication for local access to privileged accounts.	No
DISA-4r3:V-69539	The application must use multifactor (e.g., CAC, Alt. Token) authentication for local access to non-privileged accounts.	No
DISA-4r3:V-69541	The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator.	No
DISA-4r3:V-69543	The application must implement replay-resistant authentication mechanisms for network access to privileged accounts.	No
DISA-4r3:V-69545	The application must implement replay-resistant authentication mechanisms for network access to non-privileged accounts.	No
DISA-4r3:V-69547	The application must utilize mutual authentication when endpoint device non-repudiation protections are required by DoD policy or by the data owner.	No
DISA-4r3:V-69549	The application must authenticate all network connected endpoint devices before establishing any connection.	No
DISA-4r3:V-69551	Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual SSL/TLS.	No
DISA-4r3:V-69553	The application must disable device identifiers after 35 days of inactivity unless a cryptographic certificate is used for authentication.	No
DISA-4r3:V-69555	The application must enforce a minimum 15-character password length.	No
DISA-4r3:V-69557	The application must enforce password complexity by requiring that at least one upper-case character be used.	No
DISA-4r3:V-69559	The application must enforce password complexity by requiring that at least one lower-case character be used.	No
DISA-4r3:V-69561	The application must enforce password complexity by requiring that at least one numeric character be used.	No
DISA-4r3:V-69563	The application must enforce password complexity by requiring that at least one special character be used.	No

DISA-4r3:V-69565	The application must require the change of at least 8 of the total number of characters when passwords are changed.	No
DISA-4r3:V-69567	The application must only store cryptographic representations of passwords.	Yes
DISA-4r3:V-69569	The application must transmit only cryptographically-protected passwords.	Yes
DISA-4r3:V-69571	The application must enforce 24 hours/1 day as the minimum password lifetime.	No
DISA-4r3:V-69573	The application must enforce a 60-day maximum password lifetime restriction.	No
DISA-4r3:V-69575	The application must prohibit password reuse for a minimum of five generations.	No
DISA-4r3:V-69577	The application must allow the use of a temporary password for system logons with an immediate change to a permanent password.	No
DISA-4r3:V-70145	The application password must not be changeable by users other than the administrator or the user with which the password is associated.	No
DISA-4r3:V-70147	The application must terminate existing user sessions upon account deletion.	No
DISA-4r3:V-70149	The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	No
DISA-4r3:V-70151	The application, when using PKI-based authentication, must enforce authorized access to the corresponding private key.	No
DISA-4r3:V-70153	The application must map the authenticated identity to the individual user or group account for PKI-based authentication.	No
DISA-4r3:V-70155	The application, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network.	No
DISA-4r3:V-70157	The application must not display passwords/PINs as clear text.	No
DISA-4r3:V-70159	The application must use mechanisms meeting the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module.	No
DISA-4r3:V-70161	The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users).	No
DISA-4r3:V-70163	The application must accept Personal Identity Verification (PIV) credentials from other federal agencies.	No
DISA-4r3:V-70165	The application must electronically verify Personal Identity Verification (PIV) credentials from other federal agencies.	No
DISA-4r3:V-70167	The application must accept FICAM-approved third-party credentials.	No
DISA-4r3:V-70169	The application must conform to FICAM-issued profiles.	No
DISA-4r3:V-70171	Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for organization-defined auditable events.	No
DISA-4r3:V-70173	The application must have a process, feature or function that prevents removal or disabling of emergency accounts.	No
DISA-4r3:V-70175	Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications.	No
DISA-4r3:V-70177	Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications.	No
DISA-4r3:V-70179	Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions.	No
DISA-4r3:V-70181	The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions.	No
DISA-4r3:V-70183	The application must terminate all sessions and network connections when non-local maintenance is completed.	No
DISA-4r3:V-70185	The application must not be vulnerable to race conditions.	Yes
DISA-4r3:V-70187	The application must terminate all network connections associated with a communications session at the end of the session.	No
DISA-4r3:V-70189	The application must implement NSA-approved cryptography to protect classified information in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	No

DISA-4r3:V-70191	The application must utilize FIPS-validated cryptographic modules when signing application components.	Yes
DISA-4r3:V-70193	The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes.	Yes
DISA-4r3:V-70195	The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection.	Yes
DISA-4r3:V-70197	Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	No
DISA-4r3:V-70199	The application user interface must be either physically or logically separated from data storage and management interfaces.	No
DISA-4r3:V-70201	The application must set the HTTPOnly flag on session cookies.	No
DISA-4r3:V-70203	The application must set the secure flag on session cookies.	No
DISA-4r3:V-70205	The application must not expose session IDs.	No
DISA-4r3:V-70207	The application must destroy the session ID value and/or cookie on logoff or browser close.	No
DISA-4r3:V-70209	Applications must use system-generated session identifiers that protect against session fixation.	No
DISA-4r3:V-70211	Applications must validate session identifiers.	No
DISA-4r3:V-70213	Applications must not use URL embedded session IDs.	No
DISA-4r3:V-70215	The application must not re-use or recycle session IDs.	No
DISA-4r3:V-70217	The application must use the Federal Information Processing Standard (FIPS) 140-2-validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	Yes
DISA-4r3:V-70219	The application must only allow the use of DoD-approved certificate authorities for verification of the establishment of protected sessions.	No
DISA-4r3:V-70221	The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail.	No
DISA-4r3:V-70223	In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes.	No
DISA-4r3:V-70225	The application must protect the confidentiality and integrity of stored information when required by DoD policy or the information owner.	No
DISA-4r3:V-70227	The application must implement approved cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	No
DISA-4r3:V-70229	The application must use appropriate cryptography in order to protect stored DoD information when required by the information owner or DoD policy.	Yes
DISA-4r3:V-70231	The application must isolate security functions from non-security functions.	No
DISA-4r3:V-70233	The application must maintain a separate execution domain for each executing process.	No
DISA-4r3:V-70235	Applications must prevent unauthorized and unintended information transfer via shared system resources.	No
DISA-4r3:V-70237	XML-based applications must mitigate DoS attacks by using XML filters, parser options, or gateways.	No
DISA-4r3:V-70239	The application must restrict the ability to launch Denial of Service (DoS) attacks against itself or other information systems.	No
DISA-4r3:V-70241	The web service design must include redundancy mechanisms when used with high-availability systems.	No
DISA-4r3:V-70243	An XML firewall function must be deployed to protect web services when exposed to untrusted networks.	No
DISA-4r3:V-70245	The application must protect the confidentiality and integrity of transmitted information.	Yes
DISA-4r3:V-70247	The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS).	No
DISA-4r3:V-70249	The application must maintain the confidentiality and integrity of information during preparation for transmission.	No
DISA-4r3:V-70251	The application must maintain the confidentiality and integrity of information during reception.	No
DISA-4r3:V-70253	The application must not disclose unnecessary information to users.	No
DISA-4r3:V-70255	The application must not store sensitive information in hidden fields.	No

DISA-4r3:V-70257	The application must protect from Cross-Site Scripting (XSS) vulnerabilities.	Yes
DISA-4r3:V-70259	The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities.	No
DISA-4r3:V-70261	The application must protect from command injection.	Yes
DISA-4r3:V-70263	The application must protect from canonical representation vulnerabilities.	No
DISA-4r3:V-70265	The application must validate all input.	Yes
DISA-4r3:V-70267	The application must not be vulnerable to SQL Injection.	Yes
DISA-4r3:V-70269	The application must not be vulnerable to XML-oriented attacks.	Yes
DISA-4r3:V-70271	The application must not be subject to input handling vulnerabilities.	Yes
DISA-4r3:V-70273	The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	No
DISA-4r3:V-70275	The application must reveal error messages only to the ISSO, ISSM, or SA.	No
DISA-4r3:V-70277	The application must not be vulnerable to overflow attacks.	Yes
DISA-4r3:V-70279	The application must remove organization-defined software components after updated versions have been installed.	No
DISA-4r3:V-70281	Security-relevant software updates and patches must be kept up to date.	No
DISA-4r3:V-70283	The application performing organization-defined security functions must verify correct operation of security functions.	No
DISA-4r3:V-70285	The application must perform verification of the correct operation of security functions: upon system startup and/or restart; upon command by a user with privileged access; and/or every 30 days.	No
DISA-4r3:V-70287	The application must notify the ISSO and ISSM of failed security verification tests.	No
DISA-4r3:V-70289	Unsigned Category 1A mobile code must not be used in the application in accordance with DoD policy.	No
DISA-4r3:V-70291	The ISSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	No
DISA-4r3:V-70293	Application web servers must be on a separate network segment from the application and database servers if it is a tiered application operating in the DoD DMZ.	No
DISA-4r3:V-70295	The ISSO must ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	No
DISA-4r3:V-70297	The ISSO must review audit trails periodically based on system documentation recommendations or immediately upon system security events.	No
DISA-4r3:V-70301	The ISSO must report all suspected violations of IA policies in accordance with DoD information system IA procedures.	No
DISA-4r3:V-70303	The ISSO must ensure active vulnerability testing is performed.	No
DISA-4r3:V-70305	AO risk acceptance must be obtained for all public domain, shareware, freeware, and other software products/libraries with both (1) no source code to review, repair, and extend, and (2) limited or no warranty, when such products are required for mission accomplishment.	No
DISA-4r3:V-70307	Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated.	No
DISA-4r3:V-70309	The designer must ensure the application does not store configuration and control files in the same directory as user data.	No
DISA-4r3:V-70311	The ISSO must ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by following available guidance.	No
DISA-4r3:V-70313	New IP addresses, data services, and associated ports used by the application must be submitted to the appropriate approving authority for the organization, which in turn will be submitted through the DoD Ports, Protocols, and Services Management (DoD PPSM).	No
DISA-4r3:V-70317	The application must be registered with the DoD Ports and Protocols Database.	No
DISA-4r3:V-70339	The Configuration Management (CM) repository must be properly patched and STIG compliant.	No
DISA-4r3:V-70341	Access privileges to the Configuration Management (CM) repository must be reviewed every three months.	No
DISA-4r3:V-70343	A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the organization and the roles and responsibilities of the organization must be created and maintained.	No

DISA-4r3:V-70345	A Configuration Control Board (CCB) that meets at least every release cycle, for managing the Configuration Management (CM) process must be established.	No
DISA-4r3:V-70347	The application services and interfaces must be compatible with and ready for IPv6 networks.	No
DISA-4r3:V-70349	The application must not be hosted on a general purpose machine if the application is designated as critical or high availability by the ISSO.	No
DISA-4r3:V-70351	A disaster recovery/continuity plan must exist in accordance with DoD policy based on the applications availability requirements.	No
DISA-4r3:V-70353	Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The ISSO will document circumstances inhibiting a trusted recovery.	No
DISA-4r3:V-70355	Data backup must be performed at required intervals in accordance with DoD policy.	No
DISA-4r3:V-70357	Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite).	No
DISA-4r3:V-70359	Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	No
DISA-4r3:V-70361	The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	No
DISA-4r3:V-70363	The application must not contain embedded authentication data.	Yes
DISA-4r3:V-70365	The application must have the capability to mark sensitive/classified output when required.	No
DISA-4r3:V-70367	Prior to each release of the application, updates to system, or applying patches; tests plans and procedures must be created and executed.	No
DISA-4r3:V-70369	Application files must be cryptographically hashed prior to deploying to DoD operational networks.	No
DISA-4r3:V-70371	At least one tester must be designated to test for security flaws in addition to functional testing.	No
DISA-4r3:V-70373	Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state.	No
DISA-4r3:V-70375	An application code review must be performed on the application.	No
DISA-4r3:V-70377	Code coverage statistics must be maintained for each release of the application.	No
DISA-4r3:V-70379	Flaws found during a code review must be tracked in a defect tracking system.	No
DISA-4r3:V-70381	The changes to the application must be assessed for IA and accreditation impact prior to implementation.	No
DISA-4r3:V-70383	Security flaws must be fixed or addressed in the project plan.	No
DISA-4r3:V-70385	The application development team must follow a set of coding standards.	No
DISA-4r3:V-70387	The designer must create and update the Design Document for each release of the application.	No
DISA-4r3:V-70389	Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered.	No
DISA-4r3:V-70391	The application must not be subject to error handling vulnerabilities.	Yes
DISA-4r3:V-70393	The application development team must provide an application incident response plan.	No
DISA-4r3:V-70395	All products must be supported by the vendor or the development team.	No
DISA-4r3:V-70397	The application must be decommissioned when maintenance or support is no longer available.	No
DISA-4r3:V-70399	Procedures must be in place to notify users when an application is decommissioned.	No
DISA-4r3:V-70401	Unnecessary built-in application accounts must be disabled.	No
DISA-4r3:V-70403	Default passwords must be changed.	Yes
DISA-4r3:V-70405	An Application Configuration Guide must be created and included with the application.	No
DISA-4r3:V-70407	If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification.	No
DISA-4r3:V-70409	The designer must ensure uncategorized or emerging mobile code is not used in applications.	No
DISA-4r3:V-70411	Production database exports must have database administration credentials and sensitive data removed before releasing the export.	No
DISA-4r3:V-70413	Protections against DoS attacks must be implemented.	No
DISA-4r3:V-70415	The system must alert an administrator when low resource conditions are encountered.	No
DISA-4r3:V-70417	At least one application administrator must be registered to receive update notifications, or security alerts, when automated alerts are available.	No

DISA-4r3:V-70419	The application must provide notifications or alerts when product update and security related patches are available.	No
DISA-4r3:V-70421	Connections between the DoD enclave and the Internet or other public or commercial wide area networks must require a DMZ.	No
DISA-4r3:V-70423	The application must generate audit records when concurrent logons from different workstations occur.	No
DISA-4r3:V-70425	The Program Manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function.	No

CLOSE DISA APPLICATION SECURITY AND DEVELOPMENT STIG V3R10 MAPPINGS(CODESONAR V7.2)

The following table contains CodeSonar warning classes that are closely mapped to Finding IDsfrom version 3, release 10 of the DISA Application Security and Development Security STIG.

Rule	Rule Name	Supported
DISA-3r10:V-6127	The designer will ensure applications requiring user authentication are PK-enabled and are designed and implemented to support hardware tokens (e.g., CAC for NIPRNet)., CAC for NIPRNet).	No
DISA-3r10:V-6128	The designer and IAO will ensure PK-enabled applications are designed and implemented to use approved credentials authorized under the DoD PKI program.	No
DISA-3r10:V-6129	The designer will ensure the application using PKI validates certificates for expiration, confirms origin is from a DoD authorized CA, and verifies the certificate has not been revoked by CRL or OCSP, and CRL cache (if used) is updated at least daily.	No
DISA-3r10:V-6130	The designer will ensure the application has the capability to require account passwords that conform to DoD policy.	No
DISA-3r10:V-6131	The designer will ensure the application prevents the creation of duplicate accounts.	No
DISA-3r10:V-6132	The IAO will ensure all user accounts are disabled which are authorized to have access to the application but have not authenticated within the past 35 days.	No
DISA-3r10:V-6133	The IAO will ensure unnecessary built-in application accounts are disabled.	No
DISA-3r10:V-6134	The IAO will ensure default passwords are changed.	No
DISA-3r10:V-6135	The designer will ensure the appropriate cryptography is used to protect stored DoD information if required by the information owner.	Yes
DISA-3r10:V-6136	The designer will ensure data transmitted through a commercial or wireless network is protected using an appropriate form of cryptography.	Yes
DISA-3r10:V-6137	The designer will ensure the application uses the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	Yes
DISA-3r10:V-6138	The designer will ensure the application design includes audits on all access to need-to-know information and key application events.	No
DISA-3r10:V-6140	The designer and IAO will ensure the audit trail is readable only by the application and auditors and protected against modification and deletion by unauthorized individuals.	No
DISA-3r10:V-6141	The designer will ensure access control mechanisms exist to ensure data is accessed and changed only by authorized personnel.	No
DISA-3r10:V-6142	The designer will ensure all access authorizations to data are revoked prior to initial assignment, allocation or reallocation to an unused state.	No
DISA-3r10:V-6143	The designer will ensure the application executes with no more privileges than necessary for proper operation.	No
DISA-3r10:V-6144	The designer will ensure the application provides a capability to limit the number of logon sessions per user and per application.	No
DISA-3r10:V-6145	If the application contains classified data, the Program Manager will ensure a Security Classification Guide exists containing data elements and their classification.	No
DISA-3r10:V-6146	The designer will ensure the application has the capability to mark sensitive/classified output when required.	No
DISA-3r10:V-6147	The Test Manager will ensure the application does not modify data files outside the scope of the application.	No
DISA-3r10:V-6148	The designer will ensure threat models are documented and reviewed for each application release and updated as required by design and functionality changes or new threats are discovered.	No
DISA-3r10:V-6149	The designer will ensure the application does not contain source code that is never invoked during operation, except for software components and libraries from approved third-party products.	Yes
DISA-3r10:V-6151	The IAO will ensure unnecessary services are disabled or removed.	No

DISA-3r10:V-6152	The designer will ensure the application is capable of displaying a customizable click-through banner at logon which prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK"	No
DISA-3r10:V-6153	The designer will ensure the application removes authentication credentials on client computers after a session terminates.	No
DISA-3r10:V-6154	The designer will ensure the application is organized by functionality and roles to support the assignment of specific roles to specific application functions.	No
DISA-3r10:V-6155	The designer will ensure the application provides a capability to terminate a session and log out.	No
DISA-3r10:V-6156	The designer will ensure the application does not contain embedded authentication data.	Yes
DISA-3r10:V-6157	The designer will ensure the application does not contain invalid URL or path references.	Yes
DISA-3r10:V-6158	The designer will ensure the application only embeds mobile code in e-mail which does not execute automatically when the user opens the e-mail body or attachment.	No
DISA-3r10:V-6159	The designer will ensure unsigned Category 1A mobile code is not used in the application in accordance with DoD policy.	No
DISA-3r10:V-6160	The designer will ensure unsigned Category 2 mobile code executing in a constrained environment has no access to local system and network resources.	No
DISA-3r10:V-6161	The designer will ensure signed Category 1A and Category 2 mobile code signature is validated before executing.	No
DISA-3r10:V-6162	The designer will ensure uncategorized or emerging mobile code is not used in applications.	No
DISA-3r10:V-6163	The Designer will ensure the application removes temporary storage of files and cookies when the application is terminated.	No
DISA-3r10:V-6164	The designer will ensure the application validates all input.	Yes
DISA-3r10:V-6165	The designer will ensure the application does not have buffer overflows, use functions known to be vulnerable to buffer overflows, and does not use signed values for memory allocation where permitted by the programming language.	Yes
DISA-3r10:V-6166	The designer will ensure the application is not subject to error handling vulnerabilities.	Yes
DISA-3r10:V-6167	The designer will ensure application initialization, shutdown, and aborts are designed to keep the application in a secure state.	No
DISA-3r10:V-6168	The designer will ensure applications requiring server authentication are PK-enabled.	No
DISA-3r10:V-6169	The Program Manager and Designer will ensure the use of new IPs, data services, and associated ports used by the application are submitted to the appropriate approving authority for that organization, which in turn are submitted through the DoD Ports, Protocols, and Services Management (DoD PPSM).	No
DISA-3r10:V-6170	The Program Manager and designer will ensure any IA, or IA enabled, products used by the application are NIAP approved or in the NIAP approval process.	No
DISA-3r10:V-6171	The IAO will ensure recovery procedures and technical system features exist so recovery is performed in a secure and verifiable manner. The IAO will document circumstances inhibiting a trusted recovery.	No
DISA-3r10:V-6172	The IAO will ensure data backup is performed at required intervals in accordance with DoD policy.	No
DISA-3r10:V-6173	The IAO will ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	No
DISA-3r10:V-6174	The IAO will ensure production database exports have database administration credentials and sensitive data removed before releasing the export.	No
DISA-3r10:V-6197	The Program Manager will ensure a System Security Plan (SSP) is established to describe the technical, administrative, and procedural IA program and policies governing the DoD information system, and identifying all IA personnel and specific IA requirements and objectives.	No
DISA-3r10:V-6198	The Program Manager and IAO will ensure development systems, build systems, test systems, and all components comply with all appropriate DoD STIGs, NSA guides, and all applicable DoD policies. The Test Manager will ensure both client and server machines are STIG compliant.	No
DISA-3r10:V-7013	The designer will create and update the Design Document for each release of the application.	No
DISA-3r10:V-16773	The Program Manager will provide an Application Configuration Guide to the application hosting providers to include a list of all potential hosting enclaves and connection rules and requirements.	No
DISA-3r10:V-16775	The Program Manager will ensure the system has been assigned specific MAC and confidentiality levels.	No
DISA-3r10:V-16776	The Program Manager will ensure the development team follows a set of coding standards.	No

DISA-3r10:V-16777	The Program Manager will ensure COTS IA and IA enabled products, comply with NIAP/NSA endorsed protection profiles.	No
DISA-3r10:V-16778	The Program Manager will document and obtain DAA risk acceptance for all public domain, shareware, freeware, and other software products/libraries with both (1) no source code to review, repair, and extend, and (2) limited or no warranty, when such products are required for mission accomplishment.	No
DISA-3r10:V-16779	The Program Manager and designer will ensure the application is registered with the DoD Ports and Protocols Database.	No
DISA-3r10:V-16780	The Program Manager will ensure all levels of program management, designers, developers, and testers receive the appropriate security training pertaining to their job function.	No
DISA-3r10:V-16781	The Program Manager will ensure a vulnerability management process is in place to include ensuring a mechanism is in place to notify users, and users are provided with a means of obtaining security updates for the application.	No
DISA-3r10:V-16782	The Program Manager will ensure a security incident response process for the application is established that defines reportable incidents and outlines a standard operating procedure for incident response to include Information Operations Condition (INFOCON).	No
DISA-3r10:V-16783	The Program Manager will ensure procedures are implemented to assure physical handling and storage of information is in accordance with the data's sensitivity.	No
DISA-3r10:V-16784	The designer will ensure the user interface services are physically or logically separated from data storage and management services.	No
DISA-3r10:V-16785	The designer will ensure the application supports detection and/or prevention of communication session hijacking.	No
DISA-3r10:V-16786	The designer will ensure the application installs with unnecessary functionality disabled by default.	No
DISA-3r10:V-16787	The designer will ensure the application follows the secure failure design principle.	No
DISA-3r10:V-16788	The designer will ensure the application uses encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	No
DISA-3r10:V-16789	The designer will ensure private keys are accessible only to administrative users.	No
DISA-3r10:V-16790	The designer will ensure the application does not connect to a database using administrative credentials or other privileged database accounts.	No
DISA-3r10:V-16791	The designer will ensure transaction based applications implement transaction rollback and transaction journaling.	No
DISA-3r10:V-16792	The designer will ensure sensitive data held in memory is cryptographically protected when not in use, if required by the information owner, and classified data held in memory is always cryptographically protected when not in use.	No
DISA-3r10:V-16793	The designer will ensure the application properly clears or overwrites all memory blocks used to process sensitive data, if required by the information owner, and clears or overwrites all memory blocks used for classified data.	Yes
DISA-3r10:V-16794	The designer will ensure the application uses mechanisms assuring the integrity of all transmitted information (including labels and security parameters).	No
DISA-3r10:V-16795	The designer will ensure the application does not display account passwords as clear text.	No
DISA-3r10:V-16796	The designer will ensure the application transmits account passwords in an approved encrypted format.	Yes
DISA-3r10:V-16797	The designer will ensure the application stores account passwords in an approved encrypted format.	Yes
DISA-3r10:V-16798	The designer will ensure the application protects access to authentication data by restricting access to authorized users and services.	No
DISA-3r10:V-16799	The designer will ensure the application installs with unnecessary accounts disabled, or deleted, by default.	No
DISA-3r10:V-16800	The designer will ensure users' accounts are locked after three consecutive unsuccessful logon attempts within one hour.	No
DISA-3r10:V-16801	The designer will ensure locked users' accounts can only be unlocked by the application administrator.	No
DISA-3r10:V-16802	The designer will ensure the application provides a capability to automatically terminate a session and log out after a system defined session idle time limit is exceeded.	No
DISA-3r10:V-16803	The designer and IAO will ensure application resources are protected with permission sets which allow only an application administrator to modify application resource configuration files.	No
DISA-3r10:V-16804	The designer will ensure the application does not rely solely on a resource name to control access to a resource.	Yes

DISA-3r10:V-16806	The designer will ensure the web application assigns the character set on all web pages.	No
DISA-3r10:V-16807	The designer will ensure the application is not vulnerable to SQL Injection, uses prepared or parameterized statements, does not use concatenation or replacement to build SQL queries, and does not directly access the tables in a database.	Yes
DISA-3r10:V-16808	The designer will ensure the application is not vulnerable to integer arithmetic issues.	Yes
DISA-3r10:V-16809	The designer will ensure the application does not contain format string vulnerabilities.	Yes
DISA-3r10:V-16810	The designer will ensure the application does not allow command injection.	Yes
DISA-3r10:V-16811	The designer will ensure the application does not have cross site scripting (XSS) vulnerabilities.	No
DISA-3r10:V-16812	The designer will ensure the application has no canonical representation vulnerabilities.	No
DISA-3r10:V-16813	The designer will ensure the application does not use hidden fields to control user access privileges or as a part of a security mechanism.	No
DISA-3r10:V-16814	The designer will ensure the application does not disclose unnecessary information to users.	No
DISA-3r10:V-16815	The designer will ensure the application is not vulnerable to race conditions.	Yes
DISA-3r10:V-16816	The designer will ensure the application supports the creation of transaction logs for access and changes to the data.	No
DISA-3r10:V-16817	The designer will ensure the application has a capability to notify the user of important login information.	No
DISA-3r10:V-16818	The designer will ensure the application has a capability to display the user's time and date of the last change in data content.	No
DISA-3r10:V-16819	The designer will ensure development of new mobile code includes measures to mitigate the risks identified.	No
DISA-3r10:V-16820	The Release Manager will ensure the access privileges to the configuration management (CM) repository are reviewed every 3 months.	No
DISA-3r10:V-16822	The Release Manager will develop an SCM plan describing the configuration control and change management process of objects developed and the roles and responsibilities of the organization.	No
DISA-3r10:V-16823	The Release Manager will establish a Configuration Control Board (CCB), that meets at least every release cycle, for managing the CM process.	No
DISA-3r10:V-16824	The Test Manager will ensure at least one tester is designated to test for security flaws in addition to functional testing.	No
DISA-3r10:V-16825	The Test Manager will ensure the changes to the application are assessed for IA and accreditation impact prior to implementation.	No
DISA-3r10:V-16826	The Test Manager will ensure tests plans and procedures are created and executed prior to each release of the application or updates to system patches.	No
DISA-3r10:V-16827	The Test Manager will ensure test procedures are created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to ensure the system remains in a secure state.	No
DISA-3r10:V-16828	The Test Manager will ensure code coverage statistics are maintained for each release of the application.	No
DISA-3r10:V-16829	The Test Manager will ensure a code review is performed before the application is released.	No
DISA-3r10:V-16830	The Test Manager will ensure flaws found during a code review are tracked in a defect tracking system.	No
DISA-3r10:V-16831	The IAO will ensure active vulnerability testing is performed.	No
DISA-3r10:V-16832	The Test Manager will ensure security flaws are fixed or addressed in the project plan.	No
DISA-3r10:V-16833	The IAO will ensure if an application is designated critical, the application is not hosted on a general purpose machine.	No
DISA-3r10:V-16834	The IAO shall ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by the following in descending order as available: 1) commercially accepted practices, (2) independent testing results, or (3) vendor literature.	No
DISA-3r10:V-16835	The IAO will ensure at least one application administrator has registered to receive update notifications, or security alerts, when automated alerts are available.	No
DISA-3r10:V-16836	The IAO will ensure the system and installed applications have current patches, security updates, and configuration settings.	No
DISA-3r10:V-16837	The IAO will ensure the application is decommissioned when maintenance or support is no longer available.	No

DISA-3r10:V-16838	Procedures are not in place to notify users when an application is decommissioned.	No
DISA-3r10:V-16839	The IAO will ensure protections against DoS attacks are implemented.	No
DISA-3r10:V-16840	The IAO will ensure the system alerts an administrator when low resource conditions are encountered.	No
DISA-3r10:V-16841	The IAO will review audit trails periodically based on system documentation recommendations or immediately upon system security events.	No
DISA-3r10:V-16842	The IAO will report all suspected violations of IA policies in accordance with DoD information system IA procedures.	No
DISA-3r10:V-16844	The IAO will ensure back-up copies of the application software are stored in a fire-rated container and not collocated with operational software.	No
DISA-3r10:V-16845	The IAO will ensure procedures are in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	No
DISA-3r10:V-16846	The IAO will ensure a disaster recovery plan exists in accordance with DoD policy based on the Mission Assurance Category (MAC).	No
DISA-3r10:V-16847	The IAO will ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	No
DISA-3r10:V-16848	The IAO will ensure passwords generated for users are not predictable and comply with the organization's password policy.	No
DISA-3r10:V-16849	The IAO will ensure the application's users do not use shared accounts.	No
DISA-3r10:V-16850	The IAO will ensure connections between the DoD enclave and the Internet or other public or commercial wide area networks require a DMZ.	No
DISA-3r10:V-19687	The IAO will ensure web servers are on logically separate network segments from the application and database servers if it is a tiered application.	No
DISA-3r10:V-19688	The designer and the IAO will ensure physical operating system separation and physical application separation is employed between servers of different data types in the web tier of Increment 1/Phase 1 deployment of the DoD DMZ for Internet-facing applications.	No
DISA-3r10:V-19689	The designer will ensure web services are designed and implemented to recognize and react to the attack patterns associated with application-level DoS attacks.	No
DISA-3r10:V-19693	The designer will ensure execution flow diagrams are created and used to mitigate deadlock and recursion issues.	No
DISA-3r10:V-19694	The IAO will ensure an XML firewall is deployed to protect web services.	No
DISA-3r10:V-19695	The designer will ensure web services provide a mechanism for detecting resubmitted SOAP messages.	No
DISA-3r10:V-19696	The designer and IAO will ensure digital signatures exist on UDDI registry entries to verify the publisher.	No
DISA-3r10:V-19697	The designer and IAO will ensure UDDI versions are used supporting digital signatures of registry entries.	No
DISA-3r10:V-19698	The designer and IAO will ensure UDDI publishing is restricted to authenticated users.	No
DISA-3r10:V-19699	The IAO will ensure web service inquiries to UDDI provide read-only access to the registry to anonymous users.	No
DISA-3r10:V-19700	The IAO will ensure if the UDDI registry contains sensitive information and read access to the UDDI registry is granted only to authenticated users.	No
DISA-3r10:V-19701	The designer will ensure SOAP messages requiring integrity, sign the following message elements: -Message ID -Service Request -Timestamp -SAML Assertion (optionally included in messages)	No
DISA-3r10:V-19702	The designer will ensure when using WS-Security, messages use timestamps with creation and expiration times.	No
DISA-3r10:V-19703	The designer will ensure validity periods are verified on all messages using WS-Security or SAML assertions.	No
DISA-3r10:V-19704	The designer shall ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	No
DISA-3r10:V-19705	The designer shall ensure encrypted assertions, or equivalent confidentiality protections, when assertion data is passed through an intermediary, and confidentiality of the assertion data is required to pass through the intermediary.	No
DISA-3r10:V-19706	The designer will ensure the application is compliant with all DoD IT Standards Registry (DISR) IPv6 profiles.	No

DISA-3r10:V-19707	The designer will ensure supporting application services and interfaces have been designed, or upgraded for, IPv6 transport.	No
DISA-3r10:V-19708	The designer will ensure the application is compliant with IPv6 multicast addressing and features an IPv6 network configuration options as defined in RFC 4038.	No
DISA-3r10:V-19709	The designer will ensure the application is compliant with the IPv6 addressing scheme as defined in RFC 1884.	No
DISA-3r10:V-21498	The designer will ensure the application is not vulnerable to XML Injection.	No
DISA-3r10:V-21500	The designer will ensure the application does not have CSRF vulnerabilities.	No
DISA-3r10:V-21519	The Program Manager will ensure all products are supported by the vendor or the development team.	No
DISA-3r10:V-22028	The designer shall use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	No
DISA-3r10:V-22029	The designer shall use both the and elements or element when using the element in a SAML assertion.	No
DISA-3r10:V-22030	The designer will ensure the asserting party uses FIPS approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	No
DISA-3r10:V-22031	The designer shall ensure messages are encrypted when the SessionIndex is tied to privacy data.	No
DISA-3r10:V-22032	The designer shall ensure if a OneTimeUse element is used in an assertion, there is only one used in the Conditions element portion of an assertion.	No
DISA-3r10:V-47163	The release manager must ensure application files are cryptographically hashed prior to deploying to DoD operational networks.	No

BROAD DISA APPLICATION SECURITY AND DEVELOPMENT STIG V3R10 MAPPINGS (CODESONAR V7.2)

The following table contains CodeSonar warning classes that are broadly mapped to Finding IDs from version 3, release 10 of the DISA Application Security and Development Security STIG.

Rule	Rule Name	Supported
DISA-3r10:V-6127	The designer will ensure applications requiring user authentication are PK-enabled and are designed and implemented to support hardware tokens (e.g., CAC for NIPRNet)., CAC for NIPRNet).	No
DISA-3r10:V-6128	The designer and IAO will ensure PK-enabled applications are designed and implemented to use approved credentials authorized under the DoD PKI program.	No
DISA-3r10:V-6129	The designer will ensure the application using PKI validates certificates for expiration, confirms origin is from a DoD authorized CA, and verifies the certificate has not been revoked by CRL or OCSP, and CRL cache (if used) is updated at least daily.	No
DISA-3r10:V-6130	The designer will ensure the application has the capability to require account passwords that conform to DoD policy.	No
DISA-3r10:V-6131	The designer will ensure the application prevents the creation of duplicate accounts.	No
DISA-3r10:V-6132	The IAO will ensure all user accounts are disabled which are authorized to have access to the application but have not authenticated within the past 35 days.	No
DISA-3r10:V-6133	The IAO will ensure unnecessary built-in application accounts are disabled.	No
DISA-3r10:V-6134	The IAO will ensure default passwords are changed.	No
DISA-3r10:V-6135	The designer will ensure the appropriate cryptography is used to protect stored DoD information if required by the information owner.	Yes
DISA-3r10:V-6136	The designer will ensure data transmitted through a commercial or wireless network is protected using an appropriate form of cryptography.	Yes
DISA-3r10:V-6137	The designer will ensure the application uses the Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality.	Yes
DISA-3r10:V-6138	The designer will ensure the application design includes audits on all access to need-to-know information and key application events.	No
DISA-3r10:V-6140	The designer and IAO will ensure the audit trail is readable only by the application and auditors and protected against modification and deletion by unauthorized individuals.	No
DISA-3r10:V-6141	The designer will ensure access control mechanisms exist to ensure data is accessed and changed only by authorized personnel.	No
DISA-3r10:V-6142	The designer will ensure all access authorizations to data are revoked prior to initial assignment, allocation or reallocation to an unused state.	No
DISA-3r10:V-6143	The designer will ensure the application executes with no more privileges than necessary for proper operation.	No
DISA-3r10:V-6144	The designer will ensure the application provides a capability to limit the number of logon sessions per user and per application.	No
DISA-3r10:V-6145	If the application contains classified data, the Program Manager will ensure a Security Classification Guide exists containing data elements and their classification.	No
DISA-3r10:V-6146	The designer will ensure the application has the capability to mark sensitive/classified output when required.	No
DISA-3r10:V-6147	The Test Manager will ensure the application does not modify data files outside the scope of the application.	No
DISA-3r10:V-6148	The designer will ensure threat models are documented and reviewed for each application release and updated as required by design and functionality changes or new threats are discovered.	No
DISA-3r10:V-6149	The designer will ensure the application does not contain source code that is never invoked during operation, except for software components and libraries from approved third-party products.	Yes
DISA-3r10:V-6151	The IAO will ensure unnecessary services are disabled or removed.	No

DISA-3r10:V-6152	The designer will ensure the application is capable of displaying a customizable click-through banner at logon which prevents further activity on the information system unless and until the user executes a positive action to manifest agreement by clicking on a box indicating "OK"	No
DISA-3r10:V-6153	The designer will ensure the application removes authentication credentials on client computers after a session terminates.	No
DISA-3r10:V-6154	The designer will ensure the application is organized by functionality and roles to support the assignment of specific roles to specific application functions.	No
DISA-3r10:V-6155	The designer will ensure the application provides a capability to terminate a session and log out.	No
DISA-3r10:V-6156	The designer will ensure the application does not contain embedded authentication data.	Yes
DISA-3r10:V-6157	The designer will ensure the application does not contain invalid URL or path references.	Yes
DISA-3r10:V-6158	The designer will ensure the application only embeds mobile code in e-mail which does not execute automatically when the user opens the e-mail body or attachment.	No
DISA-3r10:V-6159	The designer will ensure unsigned Category 1A mobile code is not used in the application in accordance with DoD policy.	No
DISA-3r10:V-6160	The designer will ensure unsigned Category 2 mobile code executing in a constrained environment has no access to local system and network resources.	No
DISA-3r10:V-6161	The designer will ensure signed Category 1A and Category 2 mobile code signature is validated before executing.	No
DISA-3r10:V-6162	The designer will ensure uncategorized or emerging mobile code is not used in applications.	No
DISA-3r10:V-6163	The Designer will ensure the application removes temporary storage of files and cookies when the application is terminated.	No
DISA-3r10:V-6164	The designer will ensure the application validates all input.	Yes
DISA-3r10:V-6165	The designer will ensure the application does not have buffer overflows, use functions known to be vulnerable to buffer overflows, and does not use signed values for memory allocation where permitted by the programming language.	Yes
DISA-3r10:V-6166	The designer will ensure the application is not subject to error handling vulnerabilities.	Yes
DISA-3r10:V-6167	The designer will ensure application initialization, shutdown, and aborts are designed to keep the application in a secure state.	No
DISA-3r10:V-6168	The designer will ensure applications requiring server authentication are PK-enabled.	No
DISA-3r10:V-6169	The Program Manager and Designer will ensure the use of new IPs, data services, and associated ports used by the application are submitted to the appropriate approving authority for that organization, which in turn are submitted through the DoD Ports, Protocols, and Services Management (DoD PPSM).	No
DISA-3r10:V-6170	The Program Manager and designer will ensure any IA, or IA enabled, products used by the application are NIAP approved or in the NIAP approval process.	No
DISA-3r10:V-6171	The IAO will ensure recovery procedures and technical system features exist so recovery is performed in a secure and verifiable manner. The IAO will document circumstances inhibiting a trusted recovery.	No
DISA-3r10:V-6172	The IAO will ensure data backup is performed at required intervals in accordance with DoD policy.	No
DISA-3r10:V-6173	The IAO will ensure application audit trails are retained for at least 1 year for applications without SAMI data, and 5 years for applications including SAMI data.	No
DISA-3r10:V-6174	The IAO will ensure production database exports have database administration credentials and sensitive data removed before releasing the export.	No
DISA-3r10:V-6197	The Program Manager will ensure a System Security Plan (SSP) is established to describe the technical, administrative, and procedural IA program and policies governing the DoD information system, and identifying all IA personnel and specific IA requirements and objectives.	No
DISA-3r10:V-6198	The Program Manager and IAO will ensure development systems, build systems, test systems, and all components comply with all appropriate DoD STIGs, NSA guides, and all applicable DoD policies. The Test Manager will ensure both client and server machines are STIG compliant.	No
DISA-3r10:V-7013	The designer will create and update the Design Document for each release of the application.	No
DISA-3r10:V-16773	The Program Manager will provide an Application Configuration Guide to the application hosting providers to include a list of all potential hosting enclaves and connection rules and requirements.	No
DISA-3r10:V-16775	The Program Manager will ensure the system has been assigned specific MAC and confidentiality levels.	No
DISA-3r10:V-16776	The Program Manager will ensure the development team follows a set of coding standards.	No
DISA-3r10:V-16777	The Program Manager will ensure COTS IA and IA enabled products, comply with NIAP/NSA endorsed protection profiles.	No

DISA-3r10:V-16778	The Program Manager will document and obtain DAA risk acceptance for all public domain, shareware, freeware, and other software products/libraries with both (1) no source code to review, repair, and extend, and (2) limited or no warranty, when such products are required for mission accomplishment.	No
DISA-3r10:V-16779	The Program Manager and designer will ensure the application is registered with the DoD Ports and Protocols Database.	No
DISA-3r10:V-16780	The Program Manager will ensure all levels of program management, designers, developers, and testers receive the appropriate security training pertaining to their job function.	No
DISA-3r10:V-16781	The Program Manager will ensure a vulnerability management process is in place to include ensuring a mechanism is in place to notify users, and users are provided with a means of obtaining security updates for the application.	No
DISA-3r10:V-16782	The Program Manager will ensure a security incident response process for the application is established that defines reportable incidents and outlines a standard operating procedure for incident response to include Information Operations Condition (INFOCON).	No
DISA-3r10:V-16783	The Program Manager will ensure procedures are implemented to assure physical handling and storage of information is in accordance with the data's sensitivity.	No
DISA-3r10:V-16784	The designer will ensure the user interface services are physically or logically separated from data storage and management services.	No
DISA-3r10:V-16785	The designer will ensure the application supports detection and/or prevention of communication session hijacking.	No
DISA-3r10:V-16786	The designer will ensure the application installs with unnecessary functionality disabled by default.	No
DISA-3r10:V-16787	The designer will ensure the application follows the secure failure design principle.	No
DISA-3r10:V-16788	The designer will ensure the application uses encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange.	No
DISA-3r10:V-16789	The designer will ensure private keys are accessible only to administrative users.	No
DISA-3r10:V-16790	The designer will ensure the application does not connect to a database using administrative credentials or other privileged database accounts.	No
DISA-3r10:V-16791	The designer will ensure transaction based applications implement transaction rollback and transaction journaling.	No
DISA-3r10:V-16792	The designer will ensure sensitive data held in memory is cryptographically protected when not in use, if required by the information owner, and classified data held in memory is always cryptographically protected when not in use.	No
DISA-3r10:V-16793	The designer will ensure the application properly clears or overwrites all memory blocks used to process sensitive data, if required by the information owner, and clears or overwrites all memory blocks used for classified data.	Yes
DISA-3r10:V-16794	The designer will ensure the application uses mechanisms assuring the integrity of all transmitted information (including labels and security parameters).	No
DISA-3r10:V-16795	The designer will ensure the application does not display account passwords as clear text.	No
DISA-3r10:V-16796	The designer will ensure the application transmits account passwords in an approved encrypted format.	Yes
DISA-3r10:V-16797	The designer will ensure the application stores account passwords in an approved encrypted format.	Yes
DISA-3r10:V-16798	The designer will ensure the application protects access to authentication data by restricting access to authorized users and services.	No
DISA-3r10:V-16799	The designer will ensure the application installs with unnecessary accounts disabled, or deleted, by default.	No
DISA-3r10:V-16800	The designer will ensure users' accounts are locked after three consecutive unsuccessful logon attempts within one hour.	No
DISA-3r10:V-16801	The designer will ensure locked users' accounts can only be unlocked by the application administrator.	No
DISA-3r10:V-16802	The designer will ensure the application provides a capability to automatically terminate a session and log out after a system defined session idle time limit is exceeded.	No
DISA-3r10:V-16803	The designer and IAO will ensure application resources are protected with permission sets which allow only an application administrator to modify application resource configuration files.	No
DISA-3r10:V-16804	The designer will ensure the application does not rely solely on a resource name to control access to a resource.	Yes
DISA-3r10:V-16806	The designer will ensure the web application assigns the character set on all web pages.	No

DISA-3r10:V-16807	The designer will ensure the application is not vulnerable to SQL Injection, uses prepared or parameterized statements, does not use concatenation or replacement to build SQL queries, and does not directly access the tables in a database.	Yes
DISA-3r10:V-16808	The designer will ensure the application is not vulnerable to integer arithmetic issues.	Yes
DISA-3r10:V-16809	The designer will ensure the application does not contain format string vulnerabilities.	Yes
DISA-3r10:V-16810	The designer will ensure the application does not allow command injection.	Yes
DISA-3r10:V-16811	The designer will ensure the application does not have cross site scripting (XSS) vulnerabilities.	No
DISA-3r10:V-16812	The designer will ensure the application has no canonical representation vulnerabilities.	No
DISA-3r10:V-16813	The designer will ensure the application does not use hidden fields to control user access privileges or as a part of a security mechanism.	No
DISA-3r10:V-16814	The designer will ensure the application does not disclose unnecessary information to users.	No
DISA-3r10:V-16815	The designer will ensure the application is not vulnerable to race conditions.	Yes
DISA-3r10:V-16816	The designer will ensure the application supports the creation of transaction logs for access and changes to the data.	No
DISA-3r10:V-16817	The designer will ensure the application has a capability to notify the user of important login information.	No
DISA-3r10:V-16818	The designer will ensure the application has a capability to display the user's time and date of the last change in data content.	No
DISA-3r10:V-16819	The designer will ensure development of new mobile code includes measures to mitigate the risks identified.	No
DISA-3r10:V-16820	The Release Manager will ensure the access privileges to the configuration management (CM) repository are reviewed every 3 months.	No
DISA-3r10:V-16822	The Release Manager will develop an SCM plan describing the configuration control and change management process of objects developed and the roles and responsibilities of the organization.	No
DISA-3r10:V-16823	The Release Manager will establish a Configuration Control Board (CCB), that meets at least every release cycle, for managing the CM process.	No
DISA-3r10:V-16824	The Test Manager will ensure at least one tester is designated to test for security flaws in addition to functional testing.	No
DISA-3r10:V-16825	The Test Manager will ensure the changes to the application are assessed for IA and accreditation impact prior to implementation.	No
DISA-3r10:V-16826	The Test Manager will ensure tests plans and procedures are created and executed prior to each release of the application or updates to system patches.	No
DISA-3r10:V-16827	The Test Manager will ensure test procedures are created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to ensure the system remains in a secure state.	No
DISA-3r10:V-16828	The Test Manager will ensure code coverage statistics are maintained for each release of the application.	No
DISA-3r10:V-16829	The Test Manager will ensure a code review is performed before the application is released.	No
DISA-3r10:V-16830	The Test Manager will ensure flaws found during a code review are tracked in a defect tracking system.	No
DISA-3r10:V-16831	The IAO will ensure active vulnerability testing is performed.	No
DISA-3r10:V-16832	The Test Manager will ensure security flaws are fixed or addressed in the project plan.	No
DISA-3r10:V-16833	The IAO will ensure if an application is designated critical, the application is not hosted on a general purpose machine.	No
DISA-3r10:V-16834	The IAO shall ensure if a DoD STIG or NSA guide is not available, a third-party product will be configured by the following in descending order as available: 1) commercially accepted practices, (2) independent testing results, or (3) vendor literature.	No
DISA-3r10:V-16835	The IAO will ensure at least one application administrator has registered to receive update notifications, or security alerts, when automated alerts are available.	No
DISA-3r10:V-16836	The IAO will ensure the system and installed applications have current patches, security updates, and configuration settings.	No
DISA-3r10:V-16837	The IAO will ensure the application is decommissioned when maintenance or support is no longer available.	No
DISA-3r10:V-16838	Procedures are not in place to notify users when an application is decommissioned.	No
DISA-3r10:V-16839	The IAO will ensure protections against DoS attacks are implemented.	No
DISA-3r10:V-16840	The IAO will ensure the system alerts an administrator when low resource conditions are encountered.	No

DISA-3r10:V-16841	The IAO will review audit trails periodically based on system documentation recommendations or immediately upon system security events.	No
DISA-3r10:V-16842	The IAO will report all suspected violations of IA policies in accordance with DoD information system IA procedures.	No
DISA-3r10:V-16844	The IAO will ensure back-up copies of the application software are stored in a fire-rated container and not collocated with operational software.	No
DISA-3r10:V-16845	The IAO will ensure procedures are in place to assure the appropriate physical and technical protection of the backup and restoration of the application.	No
DISA-3r10:V-16846	The IAO will ensure a disaster recovery plan exists in accordance with DoD policy based on the Mission Assurance Category (MAC).	No
DISA-3r10:V-16847	The IAO will ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed.	No
DISA-3r10:V-16848	The IAO will ensure passwords generated for users are not predictable and comply with the organization's password policy.	No
DISA-3r10:V-16849	The IAO will ensure the application's users do not use shared accounts.	No
DISA-3r10:V-16850	The IAO will ensure connections between the DoD enclave and the Internet or other public or commercial wide area networks require a DMZ.	No
DISA-3r10:V-19687	The IAO will ensure web servers are on logically separate network segments from the application and database servers if it is a tiered application.	No
DISA-3r10:V-19688	The designer and the IAO will ensure physical operating system separation and physical application separation is employed between servers of different data types in the web tier of Increment 1/Phase 1 deployment of the DoD DMZ for Internet-facing applications.	No
DISA-3r10:V-19689	The designer will ensure web services are designed and implemented to recognize and react to the attack patterns associated with application-level DoS attacks.	No
DISA-3r10:V-19693	The designer will ensure execution flow diagrams are created and used to mitigate deadlock and recursion issues.	No
DISA-3r10:V-19694	The IAO will ensure an XML firewall is deployed to protect web services.	No
DISA-3r10:V-19695	The designer will ensure web services provide a mechanism for detecting resubmitted SOAP messages.	No
DISA-3r10:V-19696	The designer and IAO will ensure digital signatures exist on UDDI registry entries to verify the publisher.	No
DISA-3r10:V-19697	The designer and IAO will ensure UDDI versions are used supporting digital signatures of registry entries.	No
DISA-3r10:V-19698	The designer and IAO will ensure UDDI publishing is restricted to authenticated users.	No
DISA-3r10:V-19699	The IAO will ensure web service inquiries to UDDI provide read-only access to the registry to anonymous users.	No
DISA-3r10:V-19700	The IAO will ensure if the UDDI registry contains sensitive information and read access to the UDDI registry is granted only to authenticated users.	No
DISA-3r10:V-19701	The designer will ensure SOAP messages requiring integrity, sign the following message elements: -Message ID -Service Request -Timestamp -SAML Assertion (optionally included in messages)	No
DISA-3r10:V-19702	The designer will ensure when using WS-Security, messages use timestamps with creation and expiration times.	No
DISA-3r10:V-19703	The designer will ensure validity periods are verified on all messages using WS-Security or SAML assertions.	No
DISA-3r10:V-19704	The designer shall ensure each unique asserting party provides unique assertion ID references for each SAML assertion.	No
DISA-3r10:V-19705	The designer shall ensure encrypted assertions, or equivalent confidentiality protections, when assertion data is passed through an intermediary, and confidentiality of the assertion data is required to pass through the intermediary.	No
DISA-3r10:V-19706	The designer will ensure the application is compliant with all DoD IT Standards Registry (DISR) IPv6 profiles.	No
DISA-3r10:V-19707	The designer will ensure supporting application services and interfaces have been designed, or upgraded for, IPv6 transport.	No
DISA-3r10:V-19708	The designer will ensure the application is compliant with IPv6 multicast addressing and features an IPv6 network configuration options as defined in RFC 4038.	No

DISA-3r10:V-19709	The designer will ensure the application is compliant with the IPv6 addressing scheme as defined in RFC 1884.	No
DISA-3r10:V-21498	The designer will ensure the application is not vulnerable to XML Injection.	No
DISA-3r10:V-21500	The designer will ensure the application does not have CSRF vulnerabilities.	No
DISA-3r10:V-21519	The Program Manager will ensure all products are supported by the vendor or the development team.	No
DISA-3r10:V-22028	The designer shall use the NotOnOrAfter condition when using the SubjectConfirmation element in a SAML assertion.	No
DISA-3r10:V-22029	The designer shall use both the and elements or element when using the element in a SAML assertion.	No
DISA-3r10:V-22030	The designer will ensure the asserting party uses FIPS approved random numbers in the generation of SessionIndex in the SAML element AuthnStatement.	No
DISA-3r10:V-22031	The designer shall ensure messages are encrypted when the SessionIndex is tied to privacy data.	No
DISA-3r10:V-22032	The designer shall ensure if a OneTimeUse element is used in an assertion, there is only one used in the Conditions element portion of an assertion.	No
DISA-3r10:V-47163	The release manager must ensure application files are cryptographically hashed prior to deploying to DoD operational networks.	No