ANNEX B, APPENDIX B2

PRIORITY SECURITY CONTROL QUESTIONNAIRE
ATHLETE MANAGEMENT SYSTEM
DEPARTMENT OF NATIONAL DEFENCE

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Zoning	TA Project Manager / Developers	AC-4	How is the flow of information within the system and between interconnected systems? The system must control the flow of info within the system & between interconnected systems.	A description of each view which includes the description and evidence of flow control for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content.	☐ System views (ex. SV-1, SV-2). ☐ Operational Views (ex. OV-1, OV-5B). ☐ Security Architecture documents. ☐ Network components: FW, eCDS (diodes), IEG (gateways), Web Content Filtering proxy must be depicted in the system/operational views.
	TA Architecture/ Project Manager /BA	CA-3	Does the IT Zoning design comply with ITSG-22 and 38? Does the design also comply with DND/CAF standard; OV-1, OV-5B, SV-1, and SV-2? Describe what boundary protection device is used to establish the direct connection of an unclassified security system to an external network?	DNDAF views, SADD (system architecture design document). Approved boundary protection devices (e.g., routers, firewalls) mediate communications (i.e., information flows) between unclassified national security systems and external networks. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems.	☐ Physical Security Survey (PSS). ☐ Interconnection Security Agreement. ☐ Boundary Protection Device config file.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Zoning	OA	PE-3	What type of zone is the information system located in (Operational, Security, Restricted)? What kind of protection is in place to restrict access to the system or the system location (e.g. secure room with swipe access and key, intrusion alarms, keypad, guards etc.). Do you secure physical access devices such as keys, combinations etc.? Are those physical access devices inventoried, changed, and monitored periodically or no longer than annually? Do you maintain physical access audit logs? Are all visitors escorted and monitored when accessing the zone?	Picture or floor plan of the controlled zone, proof of satisfactory Physical Security Survey. Confirmation of physical zones (e.g. zoning map) and log data that correlates information about who has been accessing each zone.	☐ Physical Security Survey (PSS). ☐ Physical access audit logs for authorized personnel and visitors. ☐ Email from local ISSO/USS confirming the appropriate storage of keys, combinations, physical access devices, periodic changes to the keys/combinations, or when compromised.
Vulnerability Management	TA Architecture	CM-2	Is a current baseline configuration developed and maintained? [CM-2] Is the baseline configuration documented and formally reviewed?	Security CONOPS/SADD. List of Software or hardware tools that monitor any configuration changes.	☐ A listing of hardware and software comprising the information system, including configuration settings/parameters for main components/applications. ☐ Proof (screenshot) of current patch levels and frequency of patch updates for the operating system and applications installed. ☐ Processes or tools employed for monitoring configuration changes. ☐ Proof that ports, protocols, services that should not be accessible to users and devices are disabled.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Vulnerability Management	TA SSC, CFNOC, DIMEI	RA-5	Are vulnerability scans (VA) conducted monthly?	Evidence that scans are planned and conducted, analysis of reports, sharing of results, how flaws will be identified.	☐ Email from CFNOC on system on boarded to national VA services (EVAST) ☐ VA reports. ☐Vulnerability scanning results.
	TA Development	SI-2	How is flaw remediation incorporated into the config management process?	SOPs for legitimate vulnerability reporting, system flaws identified and a Remediation tested report. Platform hardening report.	☐Proof (screenshot) of the last update of AV and frequency of updates. ☐ Proof (screenshot) of current patch levels and frequency of patch updates for the operating system and applications installed.
	TA Architecture	SI-7	Are there any integrity verification tools employed on the system? What action is taken when unauthorized changes to the software, firmware, and information are detected? If hosted by SSC on GPNet - ensure RFC 48991 is reviewed and VA scanning results are sent monthly to both SSC EVSS and DIM Secur and retained.	System architecture, logs from used tools. State-of-the-practice checking mechanisms (e.g. parity checks, cyclical redundancy checks, cryptographic hashes) and associated tools can automatically monitor the integrity of the IS and hosted applications. Actions can include but not limited to restoring the data/configurations at the latest restore point, reverse changes, and apply sanctions if applicable.	☐ Proof (screenshot/logs) of integrity verification tools used (e.g. digital signatures, parity checks, cyclical redundancy checks, cryptographic hashes). ☐ Confirmation that backup of system and user information is kept in safe storage (eg. alternate site, RAID storage, virtualization, etc.). ☐ Proof of backups: screenshot of files on backup server, last backup recovery exercise date and result.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Identity and account Management	OA/TA SYS admin and App admin.	AC-2	Describe in detail the system account management procedures. The system should employ automated mechanisms to support the management of information system accounts.	Types of accounts, authorization requirements, creation, modification, deletion, disabling, least privilege, auditing of accounts, etc. The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report atypical system account usage. Screenshots demonstrating the implementation of account management.	☐ Evidence of how accounts are managed for users, admin accounts, system accounts and privileges (Screenshots, i.e. AD Group GPOs. Evidence of password configuration, session lock, etc. User roles IAW the system defined roles. ☐ Screenshot showing root login not permitted. ☐ Log samples of logins by admin and users. ☐ Proof (screenshot) showing that auditing logs for accounts are enabled. ☐ Email confirmation from local ISSO that audit logs are reviewed regularly.
	TA Project Manager or Business Analyst	AC-3	How does the system enforce approved authorizations for access based on need-to-know?	CRUD matrix, RBAC from PM or Business Analyst. Screenshots demonstrating the implementation of the control.	☐ Screenshot demonstrating that access control policies (RBAC) and access enforcement mechanisms (access control lists, access control matrices) are implemented in Active Directory (AD). ☐ screenshot of Group memberships for AD and Application configuration for access based on account membership in AD

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Identity and account Management	TA Developers, architecture	AC-6	How does the system restrict access for privileged and end users? How does the system restrict non-privileged users from performing privileged functions? The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards /countermeasures.	Organizations employ least privilege for specific duties and information systems. Applied to information system processes, this ensures that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. The information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards. Proof demonstrating the implementation. Screenshot of access management control.	☐ Proof (screenshot) of the use of least privilege for specific duties, information system processes (showing that privileged accounts are restricted to specific personnel or roles).
	TA Developers or System/Application Admin	AC-12	After how much time of inactivity is the user's session disconnected? How does the system terminate the user's session when the user is inactive?	Session termination addresses the termination of user-initiated logical sessions. A logical session is initiated whenever a user (or process acting on behalf of a user) accesses an organizational system. Such user sessions can be terminated without terminating network sessions. Session termination ends all processes associated with a user's logical session except those processes that are specifically created by the user (i.e., session owner) to continue after the session is terminated.	☐ Screenshot showing the termination of user's session after a pre-defined period of user inactivity.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Identity and account Management	TA SYS admin, App admin	IA-2	How does the system uniquely identify and authenticate end users and devices? Does the system require multi-factor authentication (MFA), if yes, how does it comply with ITSP.30.031 V3 CSE guidance and what is the authentication Level of Assurance (LoA) that will be implemented? Any application containing sensitive information must implement multifactor authentication for network access to **privileged** accounts.	Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case of multifactor authentication, some combination. Multifactor authentication can be addressed using a software-based certificate in conjunction with a username and password. Screenshots of implementation.	☐ Proof (screenshot) of uniquely identifying and authenticating organizational users. ☐ Proof of AD accounts, local accounts, SAML, and MFA used. ☐ Change to "AD accounts, local accounts, SAML, MFA" ☐ List of accounts sample with creation and expiry dates.
	TA Developers or System/Application Admin	IA-5	Will the identity of the individual, group, role, or device receiving the authenticator be verified prior to the authenticator distribution? How will the organization ensure that the authenticators have sufficient strength of mechanism for their intended use? What are the procedures in place to change and revoke an authenticator (e.g. password)? Who is allowed to perform those procedures? Who is allowed to consult the content of an authenticator? What are the minimum and maximum lifetime restrictions for an authenticator? Will there be authenticators refreshing/changing automatically?	SOP to change or revoke a password, list of the groups having access to the authenticators' content, definition of a frequency to change generic privileged accounts authenticators, configuration support snippet. Authenticators include passwords, cryptographic devices, one-time password devices, and key cards. Device authenticators include certificates and passwords. Initial authenticator content is the actual content of the authenticator (e.g., the initial password). In contrast, the requirements about authenticator content contain specific characteristics or criteria (e.g., minimum password length). Systems support authenticator management by organization-defined settings and restrictions for various authenticator characteristics	☐ Proof (screenshot) of password policies. ☐ Copy of SOPs detailing the implementation of this control.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Identity and account Management	TA Developers or System/Application Admin (Cont'd)	IA-5 (Cont'd)	(Cont'd) What security safeguards does an individual need to take? Will the generic privileged accounts (e.g. super users) used while the development phase have their authenticators changed prior to moving to the production phase? Will they be changed on a defined frequency? Will they be changed when the membership to those accounts is changed?	(Cont'd) (e.g., minimum password length, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication). Actions can be taken to safeguard individual authenticators, including maintaining possession of authenticators; not sharing authenticators with others; and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking authenticators for temporary access when no longer needed. Screenshots of implementation needed for assessment.	
Data Loss Prevention	TA/OA SYS admin and App admin.	PS-6 / PRNK-1	Is there any access agreement in place for accessing the system? At what frequency are the access agreements reviewed, updated, and re-signed (if applicable)? Verify that access to classified information requiring special protection is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; (b) Satisfy associated personnel security criteria; and (c) Have read, understood, and signed a nondisclosure agreement.	Copy of the access agreement form. Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational Systems to which access is authorized.	☐ Copy of the signed access agreement form. ☐ Account creation validation process, sys admin if critical system is SECRET. Controlled goods, SECRET enforcement, (may be done with AD flag indicating who is cleared), USS email confirming he/she vouches for all accounts. WebSCPS or SRCL with clearance confirmation.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Data Loss Prevention	TA Platform/SSC	MP-2	How does the org monitor/limit access to removable media related to the system?	Implementation of strict set of controls for media handling, detailed in the Security Orders. Systems configured to disable the ability to use mobile devices including USB and CD/DVD devices. Any technical devices used for tracking should be listed.	☐ Proof (Screenshot) of implementation of Data Loss Prevention (ex: Removable media controls, USB on the application, data at rest, encryption, etc). ☐ Logs of removable media usage validated with approved media list/custodian (ex: stormshield logs). ☐ Copy of Security Orders detailing the implementation of removable media handling.
	TA Architecture	SC-7	Does the hosted architecture and application have the capability to detect and prevent unauthorized exfiltration of information?	Boundary protection description, both Internal and External.	☐ Screenshot showing firewall rules that deny connections. ☐ Logs of boundary systems: FW, eCDS (diodes), IEG (gateways), network-based intrusion detection or prevention system, Web Content Filtering proxy. ☐ Confirmation that backup of system and user information is kept in safe storage (eg. alternate site, RAID storage, virtualization, etc.)

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Data Loss Prevention	TA/OA SYS admin and App admin.	PS-6 / PRNK-1	Is there any access agreement in place for accessing the system? At what frequency are the access agreements reviewed, updated, and re-signed (if applicable)? Verify that access to classified information requiring special protection is granted only to individuals who: (a) Have a valid access authorization that is demonstrated by assigned official government duties; (b) Satisfy associated personnel security criteria; and (c) Have read, understood, and signed a nondisclosure agreement.	Copy of the access agreement form. Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational Systems to which access is authorized.	☐ Copy of the signed access agreement form. ☐ Account creation validation process, sys admin if critical system is SECRET. Controlled goods, SECRET enforcement, (may be done with AD flag indicating who is cleared), USS email confirming he/she vouches for all accounts. WebSCPS or SRCL with clearance confirmation.
	TA Platform/SSC	MP-2	How does the org monitor/limit access to removable media related to the system?	Implementation of strict set of controls for media handling, detailed in the Security Orders. Systems configured to disable the ability to use mobile devices including USB and CD/DVD devices. Any technical devices used for tracking should be listed.	☐ Proof (Screenshot) of implementation of Data Loss Prevention (ex: Removable media controls, USB on the application, data at rest, encryption, etc). ☐ Logs of removable media usage validated with approved media list/custodian (ex: stormshield logs). ☐ Copy of Security Orders detailing the implementation of removable media handling.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Data Loss Prevention	TA Architecture	SC-7	Does the hosted architecture and application have the capability to detect and prevent unauthorized exfiltration of information?	Boundary protection description, both Internal and External.	☐ Screenshot showing firewall rules that deny connections. ☐ Logs of boundary systems: FW, eCDS (diodes), IEG (gateways), network-based intrusion detection or prevention system, Web Content Filtering proxy. ☐ Confirmation that backup of system and user information is kept in safe storage (eg. alternate site, RAID storage, virtualization, etc.)
Logging	TA Development /Architecture	SC-26	What type of decoy will be on the system? What is the procedure when an attack, a scan, or an incident is detected?	Decoys (i.e., honeypots, honeynets, or deception nets) are established to attract adversaries and to deflect attacks away from the operational systems supporting organizational missions and business functions. The procedure could be, as an example, doing an analysis of the attack(s) to identify how, by whom, and how often did we get attacked to target the response based on those results. The response could be patching the system or reporting the incident to the responsible party.	☐ Copy of the logs from the decoy system, analysis (if applicable). ☐ Copy of SOP detailing the courses of action when an attack, a scan, or an incident is detected pertaining to honeypots, honeynets?
	TA Development /Architecture/SSC	SI-3	Describe the malicious code protection installed in the system (or is it inherited from the platform/network?). During development what mechanisms are used to ensure secure coding practices are in place for applications?	Entry and exit points, updating of protection, frequency of scans, blocked/quarantined, false positive. Secure coding practices.	☐ Proof of the last update of AV and frequency of updates. ☐ Proof that secure coding practices are followed.

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Logging	TA Development /Architecture	SI-4	Does the system have the capability to detect unauthorized or malicious use of the IS?	IDS/IPS, insider and external threat, outbound comms, exfiltration of data.	☐ Proof of the System monitoring in place (proven by, for example, an email from CFNOC or other organization providing the system monitoring, (detailing the system specific IP Address and DNS included); specific use cases (ex: DDOS, Transec, APT compromise, investigations of insiders, with R&R should be included). ☐ Copy of the logs of IDS/IPS or other malicious code protection software detecting unauthorized use of the information of the system.
	OA/TA SYS admin/App admin/OA	AU-3	Does the system generate audit records containing: what type of event occurred, when it occurred, the source, the outcome of the event, and the identity of any individual associated with the event?	Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow	☐ Proof (screenshot/log files) showing WHO does WHAT, WHEN and WHERE, including hostname, user name, IP, timestamp, action performed (ex: sudo, mount, access, copy, delete).

Control Area Layers	Responsible Party	Control	ITSG-33 Definition	Expansion/Examples	Evidence Provided
Logging	OA/TA Architecture / app admin/ DAPI 6	AU-2	Describe what events are audited on the application that will support after-the-fact investigations?	Access, modifications, deletions, frequency of audits.	☐ Proof (screenshot/logs) of auditing successful and unsuccessful events such as: - password changes - failed logons - failed accesses - privileged activities or other system level access - concurrent logons from different workstations - all program initiations