Reference Sheet - Defence Policy Awareness Curriculum -May, 2014

CYBER DEFENCE BRANCH TOOL FRAMEWORK AND SERVICE DEPLOYMENT APPROVAL PROCESS WORKING AID

CSE LEGAL AND POLICY ACCOUNTABILITY			
WHEN:	**CYBER DEFENCE BRANCH**	**IPOC**	**DC ITS**
1) The Cyber Defence Branch develops a new service (e.g. [redacted] or tool framework (e.g. [redacted] [redacted]	· Must contact IPOC for policy verification to determine if there is a privacy impact	· A Service & Tool Policy Verification Form (STPV) will be signed by CDO & IPOC ensuring that intercepted private communications will be properly accounted for and the data selection process is auditable · If the tool framweork or service complies with policy, IPOC recommends DCITS approval	· Must approve deployments of all new cyber defence services and tool frameworks (whether or not they impact privacy). IPOC will provide deployment updates to DCITS in the quarterly compliance monitoring reports
2) A toolset is implemented for an existing tool framework or service (e.g. [redacted]	· Must contact IPOC to determine if the implemented changes could involve private communications, or CII	· If the implemented changes could involve private communications or CII, an updated STPV will be signed by CDO & IPOC · If the implemented changes could impact privacy, IPOC recommends DCITS approval	· Must approve all toolsets for existing services or tool frameworks that impact privacy. IPOC will provide tool deployment updates to DCITS in the quarterly compliance monitoring reports
3) A new tool or new version of a tool is implemented within an existing approved toolset (e.g. [redacted]	· No further action required	· No policy oversight required	· No approval required
4) System modifications or upgrades that have no privacy impact are implemented (e.g. script modifications for maintenance, or to improve efficiency)	· No further action required	· No policy oversight required	· No approval required
5) A non-MA tool framework or service deployed under CSEC authority	· Must ensure documented request is received · Must ensure there is no foreseeable risk of PC interception *(*Must contact IPOC if any implemented changes could involve private communications, or CII)* · If the request is from a Client other than non-GC critical infrastructure, must provide a justification of why the entity's infrastructure is of importance to GC	· No policy oversight required unless a request from a Client other than non-GC critical infrastructure is received	· No approval required unless a request from a Client other than non-GC critical infrastructure is received
CLIENT RISK ACCOUNTABILITY			
WHEN:	**CYBER DEFENCE BRANCH**	**IPOC**	**DC ITS**
1) A tool framework or service is being deployed at a new client (e.g. [redacted] at DFAIT)	· Must ensure documented request is received · Must ensure it meets policy and legal requirements (a valid STPV is in place), and is within the client's accepted risk level · If the tool or service is policy compliant and is within the client's accepted risk level, CDB recommends DCITS approval	· For activities conducted under MA, IPOC will verify that the Minister has been notified prior to deploying a tool framework or service	· Must approve deployments of all new cyber defence services and tool frameworks to ensure they are within the client's accepted risk level
2) A toolset is implemented for an existing tool framework or service (e.g. [redacted]	· Must assess if it is within the client's accepted risk level. If the change impacts the accepted risk level, consult DCITS.	· No policy oversight required	· Must ensure the client approves all changes to existing services or tool frameworks that are not within the client's pre-defined risk level
3) A new tool or new version of a tool is implemented within an existing approved toolset (e.g. [redacted]	· No further action required	· No policy oversight required	· No approval required
4) System modifications or upgrades that have no risk level impact are implemented (e.g. script modifications for maintenance, or to improve efficiency)	· No further action required	· No policy oversight required	· No approval required
5) A tool framework or service shared with non-GC clients under the client's authority	· Must highlight to client any potential risks and explain steps to follow if they require additional assistance from CSEC · If the request is from a Client other than non-GC critical infrastructure, must provide a justification of why the entity's infrastructure is of importance to GC	· No policy oversight required	· No approval required unless a request from a Client other than non-GC critical infrastructure is received

- Tool Framework: A core hardware or software module developed in order to conduct cyber defence operations (e.g. [redacted]
- Degree of Defence: Enhancements to an existing tool framework that leverages new technologies, or involves a new capability. (e.g. [redacted]
- Service: Activities undertaken in support of Mandate B. Services may deploy a tool framework to achieve an objective. (e.g. Dynamic Defence)
- Toolset: A set of software modules implemented within a tool framework to perform specific functions. (e.g. system enumeration plugins)