CYBER IMPLEMENTATION PLAN
ONLY FOR USE WITH DEFSTAN 05-138 ISSUE 3/CYBER SECURITY MODEL VERSION 3

MODERATE CYBER RISK PROFILE

Part 1: Assurance Controls and Evidence Completed by Industry

Organisation Name		
Contact Name		
Contact Email		
Contract Name		
Cyber Risk Profile		Moderate
Risk Assessment Reference (RAR)		
Supplier Assurance Questionnaire (SAQ) code (If known)		
Controls not met (paste from DCPP response email)		
Controls are ordered by security category:		
Security Governance	L01, L02, L03, M01, M02	
Security Culture and Awareness	L04, L05, L06, M03	
Information Asset Security	L07, L08, M04, M05, M06, M07	
Info-Cyber Systems Security	VL01, L09, L10, L11, L12, L13, M08, M09, M10, M11, M12, M13, M14	
Personnel Security	L14, L15, L16, M15, M16, M17	
Security Incident Management	L17	

DEFSTAN 05 -138

Only answer for controls "not met".
SAQ returns with "Not met" can be submitted providing the CIP covers those controls.

DEFCON CONTROLS (High)	Equivalent standard / controls or comment
Security Governance	
L.01 Define and implement an information security policy, related processes and procedures.	
L.02 Define and assign information security relevant roles and responsibilities.	
L.03 Define and implement a policy which addresses information security risks within supplier relationships.	
M.01 Define and implement a policy which provides for regular, formal information security related reporting.	
M.02 Define and implement a repeatable risk assessment process.	

Security Culture and Awareness

L.04 Define and implement a policy which ensures all functions have sufficient and appropriately qualified resources to manage the establishment, implementation and maintenance of information security.	
L.05 Define employee (including contractor) responsibilities for information security.	
L.06 Define and implement a policy to provide employees and contractors with information security training.	
M.03 Define and implement a repeatable risk assessment process.	
Information Asset Security	
L.07 Define and implement a policy for ensuring sensitive information is clearly identified.	
M.04 / M04a / M04b Define and implement a policy for storing, accessing, and handling sensitive information securely.	
M.05 Define and implement a policy for data loss prevention.	
M.06 Define, implement, and test a policy for regular off-line back-up of data off-site.	
L.08 Define and implement a policy to control access to information and information processing facilities.	
M.07 Ensure the organisation has identified asset owners and asset owners control access to their assets.	
Info-Cyber Systems Security	
VL.01 Maintain annually renewed Cyber Essentials Certification.	
L.09 Maintain annually renewed Cyber Essentials Scheme Plus Certification.	
L.10 Define and implement a policy to control the exchanging of information via removable media.	
L.11 Record and maintain the scope and configuration of the information technology estate.	

M.08 Define and implement a policy to assess vulnerabilities identified for which there are no countermeasures (e.g. a patch) available, undertake risk assessment and management.	
M.09 Undertake administration access over secure protocols, using multi-factor authentication.	
M.10 Define and implement a policy to monitor network behaviour and review computer security event logs for indications of potential incidents.	
L.12 Define and implement a policy to manage the access rights of user accounts.	
M.11 Define and implement a policy to monitor user account usage and to manage changes of access rights.	
M.12 Define and implement a policy to control remote access to networks and systems.	
L.13 Define and implement a policy to maintain the confidentiality of passwords.	
M.13 Define and implement a policy to control the use of authorised software.	
M.14 Define and implement a policy to control the flow of information through network borders.	
Personnel Security	
L.14 Define and implement a policy for verifying an individual's credentials prior to employment.	
M.15 Define and implement a policy for applying security vetting checks to employees	
L.15 Define and implement a process for employees and contractors to report violations of information security policies and procedures without fear of recrimination.	
L.16 Define and implement a disciplinary process to take action against employees who violate information security policies or procedures	

M.16 Undertake personnel risk assessments for all employees and contractors and ensure those with specific responsibilities for information security have sufficient appropriate qualifications and appropriate levels of appropriate experience	
M.17 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	
Security Incident Management	
L.17 Define and implement an incident management policy, which must include detection, resolution, and recovery.	

Anticipated Date of Compliance	Comment

The completed Cyber Implementation Plan (CIP) must be returned to the MoD Contracting Team (not DCPP) who will forward this on to the relevant TLB / FLC lead.