

OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER (CAJRE)

The mission of the Office of the Chief Information Security Officer (OCISO) is to administer CDC's information security program to protect CDC's information, information systems, and information technology commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency. (Approved 2/23/2012)

Office of the Director (CAJRE1)

(1) Manages and directs the activities and functions of the Office of the Chief Information Security Officer; (2) develops and maintains a CDC-wide information security program; (3) develops and maintains information security policies, procedures and control techniques to address the responsibilities assigned to the CDC under the Federal Information Security Management Act of 2002 (FISMA) and other governing statutes, regulations, and policies; (4) coordinates the professional development and operating procedures of CDC staff substantially involved in information security responsibilities; (5) assists CDC senior management concerning their FISMA responsibilities; and (6) ensures privacy management so personally identifiable information is appropriately collected, processed, stored and protected. (Approved 2/23/2012)

Operations, Analysis and Response Branch (CAJREB)

(1) Performs continuous monitoring functions including enterprise security log correlation, vulnerability and compliance scanning and risk assessments; (2) performs network monitoring, security event correlation, forensic investigations, data recovery and malware analysis; (3) develops and maintains the CDC Computer Security Incident Response Team (CSIRT); (4) performs cyber security incident reporting according to US-CERT reporting guidelines; (5) facilitates cyber security incident remediation; (6) coordinates with law enforcement agencies and participates in cyber security intelligence activities; (7) develops enterprise security architecture, firewall management, cyber security tool management and CDC information resource governance – security component; and (8) supports OCISO IT operations; and (9) performs security product research and development, evaluation and testing. (Approved 2/23/2012)

Policy and Planning Branch (CAJREC)

(1) Coordinates compliance and audit reviews; (2) develops cyber security policies and standards; (3) conducts system security tests and evaluations and identifies, assesses, prioritizes, and monitors the progress of corrective efforts for security weaknesses found in programs and systems; (4) maintains the Security Awareness Training program and coordinates significant security responsibilities and IT security training; (5) reviews and approves security and privacy related elements of OMB business cases; (6) conducts OCISO internal audit program and contract language reviews for information security and privacy act clearance decisions; (7) coordinates critical infrastructure protection continuity operations plans, data call management, E-Authentication and security requirements of CDC

information system development; (8) conducts security reviews of non-standard software for use at CDC; and (9) coordinates FISMA security milestone oversight reporting and is the Office of Inspector General and Government Accounting Office Audit Liaison. (Approved 2/23/2012)