Task Area 7 – Critical Infrastructure Protection and Information Assurance

The objective of this task area is to support the protection of critical infrastructure, assurance of agency information, and operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability, accountability, restoration, authentication, non-repudiation, protection, detection, monitoring, and event react capabilities. A comprehensive, but not limited, sampling of work to be performed under this task area is shown below:

a) Cyber Security

b) Critical Infrastructure Asset Identification and Configuration Management Databases

c) Information Assurance of Critical Infrastructure

d) Risk Management (Vulnerability Assessment and Threat Identification)

e) Facility Protection Planning

f) Information Systems Security

g) Security Operations Center Development and Operations Management

h) Application Security

i) Disaster Recovery

j) Critical Infrastructure Continuity and Contingency Planning

k) Incident Response Planning and Execution

l) Security Certification and Accreditation

m) Training and Awareness Programs

n) Exercises and Simulation

o) Federal Information Security Management Act (FISMA) Implementation Support

p) Health Insurance Portability and Accountability Act Implementation Support

q) Cryptographic Support and Services

r) Record Management

s) Public Key Infrastructure

t) Trusted Internet Connections implementation

u) Security Review and Analysis of Automated Information Systems

v) Identity Management and Assurance

w) Intelligent, Automated Data Collection and Analysis

x) IT Forensics and eDiscovery