



# Example of Cyber Operations Job Description

Powered by [www.VelvetJobs.com](http://www.VelvetJobs.com)

Our company is growing rapidly and is hiring for a cyber operations. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

## Responsibilities for cyber operations

- Identify unauthorized activity against USTRANSCOM information systems and networks on NIPRNet and SIPRNet and initiate appropriate incident response actions
- Perform installation of intrusion detection monitoring and incident management tools IAW USTRANSCOM processes, including requesting/coordinating hardware/software procurement (including lifecycle upgrades)
- Perform the day-to-day mission execution of the intrusion detection monitoring and incident management and response activity
- Perform the day-to-day operation and maintenance of the intrusion detection monitoring and incident management tool suite
- Document changes to intrusion detection monitoring and incident management tools (e.g., software installs, patching, software configuration changes, ) in accordance with Change Management policies and provide configuration management data on all of its managed systems according to the schedule and format directed by the Government
- Collect and provide the Government with monthly metrics on intrusion detection monitoring and incident management activity
- Provide cyber threat analysis support to USTRANSCOM's Cyber Security Service Provider (CSP) and Joint Cyber Center (JCC) Defensive Cyber Operations (DCO) missions on-site at Scott AFB during normal duty hours and on-call after duty hours with a one (1) hour response time to begin work
- Collect, analyze, and report on security events that affect the operation of

and CSP subscriber enclaves, and for systems hosted elsewhere for which USTRANSCOM is the authorizing official

- Collect, analyze, and report security events that affect the operation of USTRANSCOM's mission environment and identified Cyber-Key Terrain (C-KT)
- Collect and provide the Government with monthly metrics on cyber threat analysis activity

## Qualifications for cyber operations

- CISM and CISSP designations are mandatory
- Extensive knowledge of networking protocols
- Detailed Internet, networking, and computer knowledge (Software & Hardware)
- Manage setting up lab for test event initiation, recovery and roll-back
- Minimum 2 years of experience building and supervising a Test Lab
- Must be proficient in developing and presenting, both verbally and in writing, highly technical information and presentations to non-technical audiences at all levels of the organization