Cyber Guard 15 Fact Sheet

Cyber Guard 15 Overview:
Cyberspace and critical infrastructure operators and experts from over 100 organizations, spanning government, academia, industry and allies, participated in the fourth annual Cyber Guard exercise, June 8-26th. U.S. Cyber Command, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) co-led the exercise. Participants rehearsed a whole-of-nation response to destructive cyber attacks against U.S. critical infrastructure. The Joint Staff J7 (Force Development) hosted Cyber Guard 15 in a state-of-the-art facility in Suffolk, VA designed to support a wide range of military tests and exercises.

Cyber Guard Objectives (are to):

- Improve the ability of our forces to defend DoD information networks, secure DoD data, and mitigate risks to DoD missions.
- Support DoD's mission to be prepared to defend the U.S. homeland and vital interests from disruptive or destructive cyberattacks of significant consequence.
- Improve shared situational awareness between government agencies, private sector and allied partners.
- Improve capabilities and processes to rapidly detect and effectively respond to a destructive or disruptive cyber attack impacting U.S. critical infrastructure, which requires whole-of-nation effort.
- Strengthen partnerships within government, allies and the private sector. Partnerships are vital to deter and respond to shared threats.
- Build and maintain ready forces and capabilities within the Department of Defense to conduct cyberspace operations. Within the exercise, U.S. Cyber Command assesses the proficiency and readiness of Cyber Mission Force teams.
- Continue efforts to build a Persistent Training Environment for cyberspace forces across the Department of Defense. This Persistent Training Environment includes a closed exercise network, training event planning, management and assessment, a live expert opposing force and transport layer to enable distributed participation in the environment. This Persistent Training Environment will be accessible to other U.S. government departments, allies and other partners and will set the foundation for whole-of-nation, full-spectrum cyberspace operations training.

Cyber Guard 15 Participants: More than 1000 participants including active duty Army, Navy, Marines, Air Force and Coast Guard as well as National Guard and Reserve units and personnel.

- DHS, FBI, and the Federal Aviation Administration (FAA).
- Members of USCYBERCOM, including the Joint Operations Center, Cyber National Mission Force Headquarters, Joint Force Headquarters-DOD Information Networks (the latter of which is responsible for coordinating the operation and defense of the DODIN), and the Cyber Mission Force - the maneuver elements of the joint force in cyberspace.
- U.S. Northern Command, U.S. Strategic Command.
- 17 Cyber Protection Teams (CPTs): One of three segments of the Cyber Mission Force, CPTs are deployed throughout the U.S. to support various DOD combatant commands, services and agencies. CPTs defend the DoDIN and help support the DOD's requirement to provide intelligence, assessments and active-duty capabilities to defend the nation.
- Computer Network Defense Service Teams (CND-SPs) from the Army, Navy, Air Force, Marines, and Coast Guard. CND-SPs provide the initial protect, detect, and respond mission to cyber incidents.
- National Guard teams from 16 states.
- Service Component Commands (Army Cyber, U.S. Navy Fleet Cyber, Marine Forces Cyber, Air Force Cyber, and Coast Guard Cyber Command).
- Reserve personnel from Army, Navy, Marines and Air Force.
- 12 State Joint Operations Centers/Emergency Operations Centers/Fusion Centers.
- Intelligence Community representatives including the National Security Agency.
- Three private industry Information Sharing and Analysis Centers, which provide their respective CI/KR members with information for risk management and incident alert and response.
    - Financial Services ISAC
    - Electricity Sector ISAC
    - Multi-State ISAC
- The first Information Sharing and Analysis Organization representing eight of the 16 critical infrastructures.
- Private industry partners from the financial and energy sectors.
- The National Cybersecurity and Communications Integration Center, Office of Cybersecurity and Communications, National Protection and Programs Directorate, DHS.
- The Office of Infrastructure Protection, National Protection and Programs Directorate, DHS.

Participants included more than 1000 individuals serving in various roles including 14 teams provided 'over-the-shoulder' training, assistance, and advising to private industry and DoD mission owners of Industrial Control Systems (ICS) commonly found in critical infrastructure facilities. Hands-on instruction and exercise scenarios were conducted on a classified (SECRET) closed network environment which emulates both DoD and non-DoD networks. Blue Team "friendly forces" worked to defend critical infrastructure networks and respond to a range of incidents. A live, expert opposing force (OPFOR) replicated a range of adversaries seeking to disrupt critical US infrastructure.

Cyber Guard 15 Phases:

- Phase 1: State and Federal support to private, municipal, and state owned critical infrastructure/key resources executed in accordance with the National Response Framework and Defense Support to Civil Authorities.
- Phase 2: Defense support to Federal agencies to include the Federal Aviation Administration.
- Phase 3: Focused training and certification of DoD cyber teams and joint cyber headquarters elements.

Cyber Guard History:

- Cyber Guard is an evolving exercise, continually expanding to meet the demands of the Department of Defense and the nation.
- Cyber Guard 12-1 was developed to foster coordinated cyberspace incident responses between the Federal and state governments, exploring the National Guard's potential as an enabler and "force multiplier" in the cyberspace domain.
- Cyber Guard 13-1 expanded in scope as a collaborative, tactical-level exercise focused on state and national defensive cyberspace operations and included Federal Bureau of Investigation and Department of Homeland Security National Cybersecurity and Communications Integration Center (NCCIC) participation.
- Cyber Guard 14-1 improved realism by requiring teams to report information to state and Federal cyber centers outside of the exercise network. Six state Joint Operations Centers (JOCs), the DHS NCCIC watch floor, and the FBI Cyber Task Force and National Cyber Intelligence Joint Task Force (NCIJTF) were actively engaged throughout the exercise.
- Cyber Guard 15 is the fourth in this series, and its expanded scope reflects the growing requirement to improve preparedness across government and the private sector. The addition of private sector participation, coordinated with the DHS Office of Infrastructure Protection Sector Outreach & Programs Division, represents a shift from a whole-of-government to whole-of-nation approach to cybersecurity preparedness and response. Cyber Guard 15 also provided another opportunity for USCYBERCOM to assess proficiency and operational readiness of its CMF teams.

Primary U.S. Government Roles and Responsibilities:

- Responsibility for protecting and defending U.S. critical infrastructure in cyberspace is a shared response across Federal, state and tribal governments and the private sector.
- At the Federal level, the primary responsibility is shared by Department of Homeland Security, Department of Justice through the Federal Bureau of Investigation, and Department of Defense:
    - DHS is responsible for the security of federal networks, promoting information sharing, and protection of U.S. critical infrastructure through preparedness and response measures.
    - The FBI is responsible for response to, and investigation of, cyber incidents.
    - The Department of Defense is responsible for:
        - Operation and defense of DoD information networks, protection of DoD data, and assurance of DoD missions; and
        - Defense of the U.S. homeland and vital interests from disruptive or destructive cyberattacks of significant consequence
- State governments are responsible for the public health and welfare of residents.

In Cyber Guard, participants leveraged the proven framework and methods for response to domestic incidents, including defense support to civil authorities, for the response to the scenario of a destructive cyber attack against U.S. critical infrastructure.

U.S. Cyber Command Mission:

- Provide mission assurance through the operation and defense of the Department of Defense information environment.
- Deter or defeat strategic threats to U.S. interests and infrastructure.
- Support the achievement of joint force commander objectives.