July 31, 2008

CYBER ANALYSIS AND WARNING

DHS Faces Challenges in Establishing a Comprehensive National Capability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-08-588, a report to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Cyber analysis and warning capabilities are critical to thwarting computer-based (cyber) threats and attacks. The Department of Homeland Security (DHS) established the United States Computer Emergency Readiness Team (US-CERT) to, among other things, coordinate the nation's efforts to prepare for, prevent, and respond to cyber threats to systems and communications networks. GAO's objectives were to (1) identify key attributes of cyber analysis and warning capabilities, (2) compare these attributes with US-CERT's current capabilities to identify whether there are gaps, and (3) identify US-CERT's challenges to developing and implementing key attributes and a successful national cyber analysis and warning capability. To address these objectives, GAO identified and analyzed related documents, observed operations at numerous entities, and interviewed responsible officials and experts.

What GAO Recommends

GAO is making 10 recommendations to the Secretary of Homeland Security to implement key attributes and address challenges. DHS concurred with 9 recommendations. It took exception to GAO's recommendation to ensure distinct and transparent lines of authority and responsibilities between its organizations, stating it had done this in a concept-of-operations document. However, this document is still in draft, and DHS has not established a date for it to be finalized and implemented.

To view the full product, including the scope and methodology, click on GAO-08-588. For more information, contact Dave Powner at 202-512-9286 or pownerd@gao.gov.

What GAO Found

Cyber analysis and warning capabilities include (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. GAO identified 15 key attributes associated with these capabilities, as shown in the following table:

Key Attributes of Cyber Analysis and Warning

Capability	Attribute
Monitoring	• Establish a baseline understanding of network assets and normal network traffic volume and flow • Assess risks to network assets • Obtain internal information on network operations via technical tools and user reports • Obtain external information on threats, vulnerabilities, and incidents • Detect anomalous activities
Analysis	• Verify that an anomaly is an incident (threat of attack or actual attack) • Investigate the incident to identify the type of cyber attack, estimate impact, and collect evidence • Identify possible actions to mitigate the impact of the incident • Integrate results into predictive analysis of broader implications or potential future attack
Warning	• Develop attack and other notifications that are targeted and actionable • Provide notifications in a timely manner • Distribute notifications using appropriate communications methods
Response	• Contain and mitigate the incident • Recover from damages and remediate vulnerabilities • Evaluate actions and incorporate lessons learned

Source: GAO analysis.

While US-CERT's cyber analysis and warning capabilities include aspects of each of the key attributes, they do not fully incorporate all of them. For example, as part of its monitoring, US-CERT obtains information from numerous external information sources; however, it has not established a baseline of our nation's critical network assets and operations. In addition, while it investigates if identified anomalies constitute actual cyber threats or attacks as part of its analysis, it does not integrate its work into predictive analyses. Further, it provides warnings by developing and distributing a wide array of notifications; however, these notifications are not consistently actionable or timely.

US-CERT faces a number of newly identified and ongoing challenges that impede it from fully incorporating the key attributes and thus being able to coordinate the national efforts to prepare for, prevent, and respond to cyber threats. The newly identified challenge is creating warnings that are consistently actionable and timely. Ongoing challenges that GAO previously identified, and made recommendations to address, include employing predictive analysis and operating without organizational stability and leadership within DHS, including possible overlapping roles and responsibilities. Until US-CERT addresses these challenges and fully incorporates all key attributes, it will not have the full complement of cyber analysis and warning capabilities essential to effectively performing its national mission.