



### Why This Matters

The Department of Homeland Security's (DHS) ability to perform mission essential functions continuously rests upon the availability and integrity of its mission essential systems and critical communications assets. The objective of our audit was to determine the progress that the Office of the Chief Information Officer has made in carrying out its continuity planning roles and developing contingency planning strategies for routine backup of critical data, programs, documentation, and personnel for recovery after an interruption.

### DHS Response

The Chief Information Officer concurred with eight recommendations and has begun to take actions to implement them.

## DHS Needs To Strengthen IT Continuity and Contingency Planning Capabilities

### What We Determined

DHS has made progress toward implementing effective disaster recovery capabilities at the Department's two enterprise data centers. Specifically, it has established a list of disaster recovery services that DHS components can procure for their systems. Additionally, the enterprise data centers now have disaster recovery enclaves that provide backup capabilities that allow continued minimum operations in the event of a disaster. Although DHS has strengthened its disaster recovery capabilities at the Enterprise Data Centers, more work is needed. The Office of the Chief Information Officer's inadequate continuity and contingency planning increases the risk that the Department may not be able to respond effectively in case of an emergency or disaster. Specifically, the Department does not have a headquarters information technology (IT) disaster recovery plan that details the transition of its headquarters critical information systems and communication assets from the primary site to the alternate site. Also, the Office of the Chief Information Officer has not established policy that requires mission essential systems to be rated as having "high" criticality in accordance with the National Institute of Standards and Technology's Federal Information Processing Standards Publication 199. Finally, because of contingency planning weaknesses, all seven of the Department's enterprise mission essential systems that we reviewed are at risk of not having capabilities to react to emergency events, to restore essential business functions if a disruption occurs, and to resume normal operations.

### What We Recommend

We made nine recommendations to the Office of the Chief Information Officer to improve the Department's IT continuity planning and its development of contingency strategies.

### For Further Information:

Contact our Office of Public Affairs at (202)254-4100, or email us at [DHS-OIG.OfficePublicAffairs@oig.dhs.gov](mailto:DHS-OIG.OfficePublicAffairs@oig.dhs.gov)