May 2014

NUCLEAR SECURITY

NNSA Should Establish a Clear Vision and Path Forward for Its Security Program

GAO Highlights

Highlights of GAO-14-208, a report to congressional requesters

Why GAO Did This Study

NNSA, a semiautonomous agency in DOE, is responsible for protecting sensitive assets, including classified information and plutonium used at its contractor-operated sites to carry out nuclear weapons-related missions. Contractors provide security at NNSA's sites under the direction and oversight of DNS, NNSA field offices, and DOE. In response to rising security costs and other concerns, from 2009 to 2012, DOE and NNSA initiated various reforms to identify and eliminate potentially unnecessary security costs; realign security requirements that may be impeding sites' productivity; and streamline federal oversight. After a serious security breach at its Y-12 site in July 2012, however, NNSA reexamined some of its reforms and considered additional actions.

GAO was asked to examine NNSA's security reforms. GAO examined (1) DOE, NNSA, and contractors' implementation of the 2009 to 2012 security reforms, including any benefits or drawbacks they identified for NNSA and its sites, and (2) NNSA's actions or plans to improve security performance and oversight after the Y-12 security breach. GAO reviewed DOE and NNSA documents and interviewed DOE and NNSA headquarters officials and NNSA field office officials and contractors at the seven NNSA sites.

What GAO Recommends

GAO recommends NNSA develop a clear vision and path forward for its security program and an implementation strategy including regular monitoring. NNSA agreed with the recommendation.

View GAO-14-208. For more information, contact David C. Trimble at (202) 512-3841 or trimbled@gao.gov.

What GAO Found

Implementation of security reforms from 2009 to 2012 generally varied among National Nuclear Security Administration (NNSA) sites. According to Department of Energy (DOE) and NNSA officials and contractors, some of these efforts helped manage security costs and enhance productivity, among other benefits, but may also have increased security risks and reduced security performance at the Y-12 National Security Complex (Y-12) in Tennessee and other NNSA sites, depending on how the sites implemented the reforms. For example, NNSA's headquarters Office of Defense Nuclear Security (DNS) conducted in-depth reviews at sites and recommended elimination of certain expenditures, for a potential savings of $53 million. However, not all of these cuts were implemented by the sites, and NNSA has limited quantifiable data on the benefits of these or other actions. NNSA officials and contractors at several sites also noted that some recommendations made during the reviews may have encouraged inappropriate risks by, for example, calling for cuts in what some of the officials or contractors described as critical protective force posts and patrols. Other actions to implement the reforms may also have increased risks, particularly at Y-12. Specifically, NNSA issued its own security policies in place of DOE's security directives, giving NNSA's contractors greater authority to make security decisions and accept risks. At the same time, DOE and NNSA scaled back on their security inspections and increased their reliance on contractors to self-monitor and self-evaluate their security performance at NNSA sites. Particularly at Y-12, some of these actions to implement the 2009 to 2012 reforms may have increased risks and reduced security performance. Some of the actions at Y-12 to implement the reforms were also later identified by DOE and NNSA as being among the causes of that site's July 2012 security breach.

After the Y-12 security breach, NNSA took a number of actions designed to improve its security performance and oversight but did so without first developing a clear vision and path forward for its security program and an implementation strategy, including milestones and responsibilities for carrying them out. For example, NNSA initiated actions to reinstate the DOE security directives, which it had previously replaced with its own security policies; started, then discontinued, a security inspection program; and reorganized its headquarters security office twice. According to some DOE and NNSA officials, NNSA undertook these and other actions without first developing the NNSA security "road map" that its Security Task Force had called for in 2012, as a priority recommendation after the Y-12 breach. More specifically, the task force had recommended that NNSA develop a clear vision and path forward for its security program and an implementation strategy, including regular monitoring, to help ensure that its actions will lead to sustainable solutions—a recommendation that mirrors effective practices GAO has previously identified for successfully implementing and sustaining management improvement initiatives. Without a road map for its security program, NNSA may prolong what some of its own officials have described as a "chaotic" or "dysfunctional" period in NNSA's security program since the 2012 security breach. In addition, NNSA risks putting in place short-lived or ineffective responses to its security problems, on which GAO and others have reported for more than a decade.