Federal agencies have reported mixed progress in securing their systems and implementing key security activities. For example, in fiscal year 2009, agencies collectively reported an increasing percentage of personnel receiving security awareness training and specialized security training, but a decreasing rate of implementation for other key activities when compared to fiscal year 2008. In addition, federal systems continued to be afflicted by persistent control weaknesses. Almost all of the 24 major federal agencies had information security weaknesses in five key control categories, as illustrated in the figure below.

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented key elements of an agencywide information security program, as required by FISMA. As a result, they may be at increased risk of unauthorized disclosure, modification, and destruction of information or disruption of mission critical operations. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Opportunities exist to enhance federal cybersecurity through a concerted response to safeguarding systems that include several components. First, agencies can implement the hundreds of recommendations GAO and inspectors general have made to resolve control deficiencies and information security program shortfalls. In addition, OMB’s continued efforts to improve reporting and oversight as recommended by GAO could help assess agency programs. Finally, the White House, OMB, and certain federal agencies have undertaken several governmentwide initiatives that are intended to enhance information security at federal agencies.