TREY GOWDY, SOUTH CAROLINA
CHAIRMAN

ONE HUNDRED FIFTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5074
MINORITY (202) 225–5051
http://oversight.house.gov

Opening Statement
Ranking Member Gerald E. Connolly
Hearing on "GAO High Risk Focus: Cybersecurity"
July 25, 2018

Chairman Meadows, Chairman Hurd, and Ranking Member Kelly, from the FITARA Scorecard hearings to hearings on the risks posed by legacy IT systems which led to passage of the Modernizing Government Technology (MGT) Act, our two subcommittees have long been concerned about the threats posed by federal cybersecurity vulnerabilities. Despite our efforts to bring attention to this urgent security priority, the situation has deteriorated and now the lights are blinking red. In fact, the federal cybersecurity posture is so problematic that the Government Accountability Office (GAO) has taken the rare step in issuing a special mid-cycle High Risk Report on cybersecurity to provide Congress with a thorough look at the federal government's approach to cybersecurity.

What makes the federal IT environment so difficult to secure is a broad array of risks agencies face which include hard to patch legacy IT systems, escalating and emerging threats from around the globe, evolving and increasingly more destructive methods of cyberattacks, and even insider threats – whether purposeful or accidental – from those with authorized access to agency networks. Congress is often focused on cybersecurity at defense and national security agencies, and agencies with known sensitive information such as the Social Security Administration or the Internal Revenue Service (IRS). However, every federal agency holds sensitive information that if inappropriately accessed and disclosed could threaten our national security, economic well-being, or public health. For example, a successful cyber-attack at the Department of Education could expose the name, address, social security number, driver's license number, and tax information of every single financial aid applicant and their parents. A breach at the Food and Drug Administration (FDA) would result in exposure of some of the most valuable proprietary business information used in approving drugs for market. Significant economic damage to companies regulated by the FDA could result if this information is not adequately protected.

As GAO will lay out at today's hearing, the Trump Administration has failed to establish a comprehensive cybersecurity strategy. Despite a Presidential executive order in May 2017, a National Security Strategy last December, and a DHS Cybersecurity Strategy in May, the documents lacked clearly defined roles and responsibilities for key agencies such as the Department of Homeland Security (DHS), the Department of Defense (DOD), and the Office of Management and Budget (OMB). As GAO notes, the documents did not include key guidance for decision makers for allocating resources, defining policies, and helping to ensure

accountability. Without this information, the federal government cannot foster effective coordination or hold agencies accountable for carrying out planned activities. Ultimately, these documents need to be useful for day-to-day decision-making or else they end up gathering dust on shelves in the subbasements of executive branch agencies.

Given the challenge federal agencies face in securing federal networks, the complexity and evolving nature of cyber threats, and the risk to national and economic security, it is disconcerting that this Administration has taken action to make it more difficult for federal agencies to confront the cyber threat. This past May, the White House eliminated the position of cybersecurity coordinator on the National Security Council (NSC). This position was responsible for developing policy to defend against cyber-attacks and coordinating cybersecurity policy across the federal government. In a memorandum, National Security Adviser John Bolton said the position was no longer necessary because lower-level staff had already made cybersecurity issues a "core function" of the president's national security team. This decision does nothing but leave the White House and the federal government short-handed in the face of increasing cybersecurity threats.

I urge the Administration to take sustained action to implement GAO's recommendations and issue a cybersecurity plan that includes milestones and performance measures that can gauge agency progress. Additionally, I strongly advise the National Security Advisor to reconsider the reckless decision to eliminate the cybersecurity coordinator position at the NSC. As the federal government and the nation's critical infrastructure becomes increasingly dependent on IT systems and electronic data, it becomes more urgent for agencies – led by the White House – to address weaknesses in their IT systems and secure their networks.

Contact: Aryele Bradford, Deputy Communications Director, (202) 226-5181.