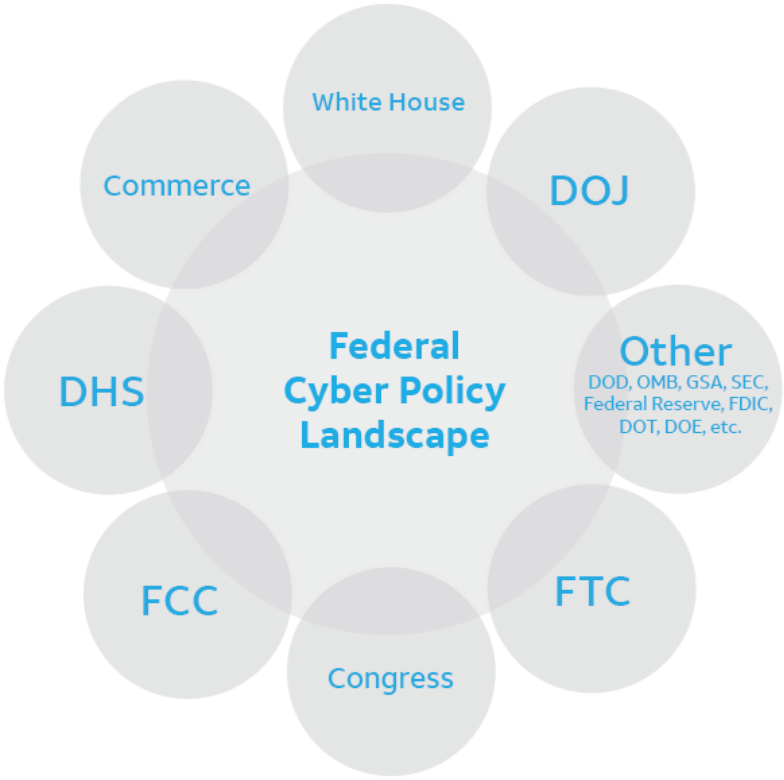
Existing Cybersecurity Governance

The communications sector has a long history of working cooperatively and productively with the federal government to prevent and respond to cybersecurity breaches.

Despite the success of this public-private partnership model, some advocate for imposing rigid cybersecurity regulations on industry. **This would be a mistake.** The inherently backward-looking nature of regulation is ill-suited for the challenges of cybersecurity. **State specific requirements are also ill advised**, since differing rules in each state increase the risk of fragmentation and force companies into a "least common denominator" approach that reduces, rather than enhances, security.

Organizations and initiatives built on a **public-private partnership model** have proven most effective in providing the policy, planning, and operations framework necessary for a coordinated and effective response to cyber incidents. Three processes are particularly important to the communications sector:

Today, **there are dozens of governmental bodies and initiatives** involved in cybersecurity policy:



Representative diagram. Not intended to be all inclusive of agency roles or activities.

- The **National Security Telecommunications Advisory Committee (NSTAC),** comprised of about 30 chief executives from the telecommunications industry, makes **policy** recommendations to the President on how to maintain a reliable, secure, and resilient national communications posture.

- The **Communications Sector Coordinating Council (C-SCC),** comprised of about 40 members from all parts of the communications industry, collaborates with designated federal agencies, including the Department of Homeland Security (DHS), to **plan** activities designed to improve the physical and cyber security of critical infrastructure.
    - The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides guidance for how companies can assess and improve their ability to prevent, detect, and respond to cyber-attacks.

- The **National Coordinating Center for Communications (NCC**) Communications Information Sharing and Analysis Center (C-ISAC), comprised of about 50 communications industry member companies, is an **operations** center that continuously monitors cyber threats and incidents and facilitates the exchange of this information with DHS and other agencies.

The increasing complexity and sophistication of cyber attacks requires diligence on the part of both the public and the private sector. Public-private partnerships have proven to be the most effective framework in helping to keep our nation's communications networks safe and secure.