RESEARCH

Survey: Security and Federal Government

A Survey of IT Security Stakeholders Across the Public and Private Sector

FALL 2021

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Research Goal

The primary research goal was to examine recent actions taken by the federal government to improve cybersecurity.

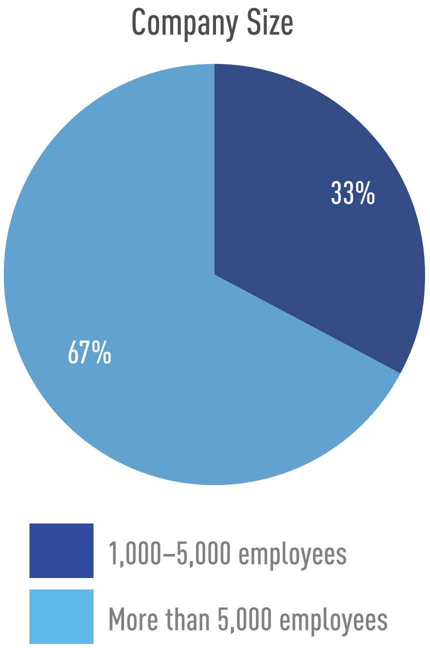
Methodology

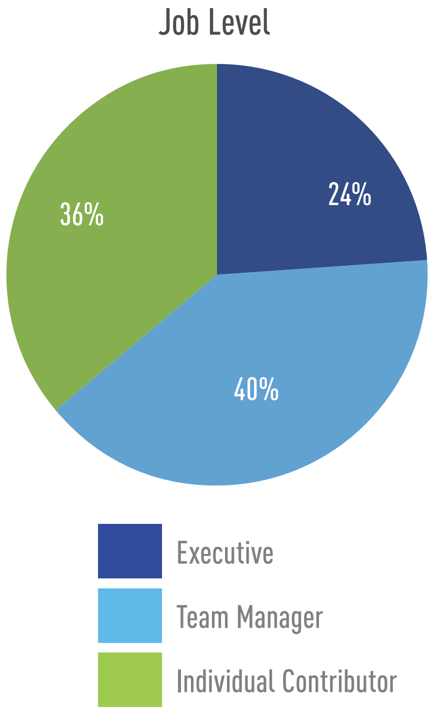
Independent sources of IT security professionals were invited to participate in an online survey. A variety of questions were asked on topics related to overall security as well as topics specific to federal government . Responses were captured between September 20 and 27, 2021.

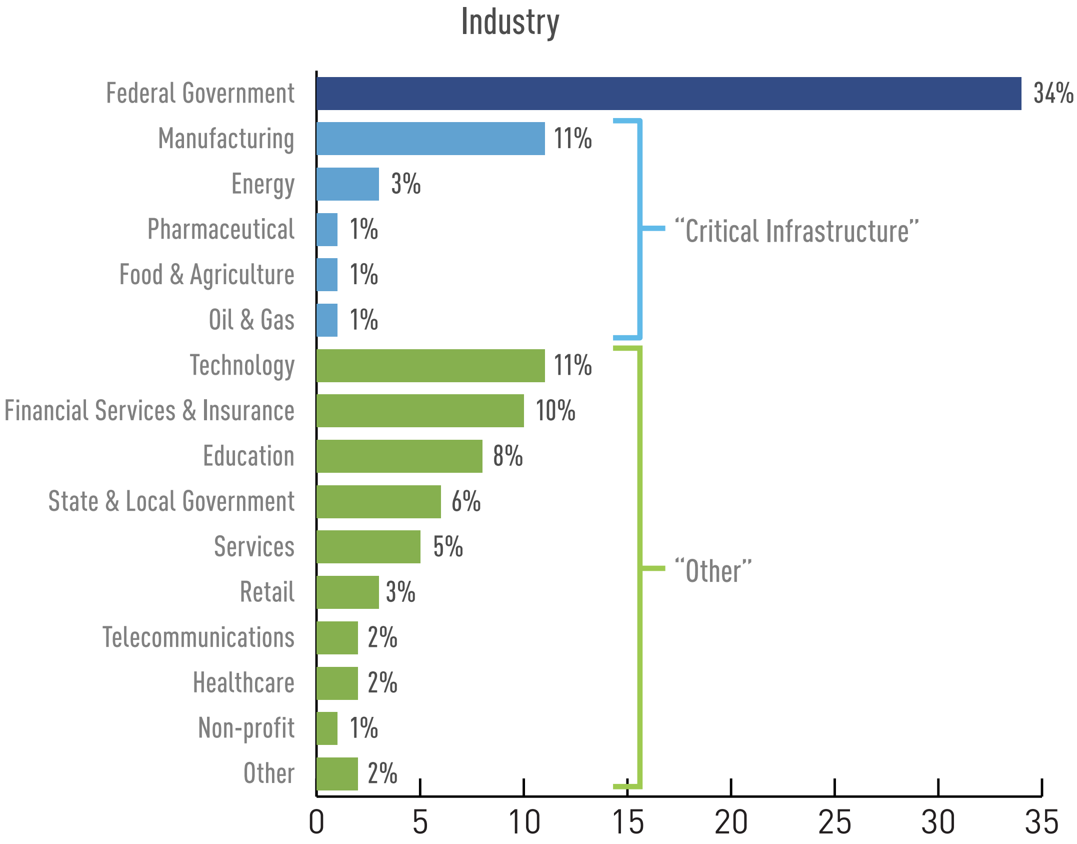
Participants

A total of 306 qualified individuals completed the survey including 103 that worked for a United States federal government agency. All lived in the United States and had responsibility for IT security at an organization with more than 1,000 employees.

COMPANIES REPRESENTED

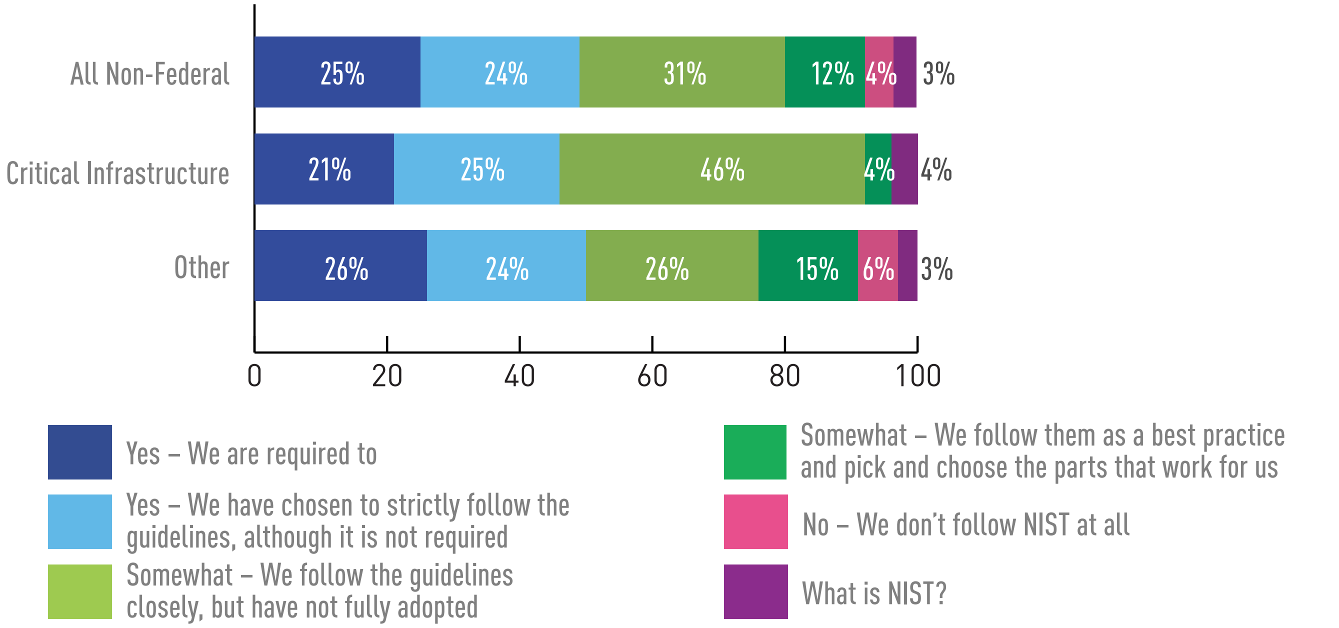






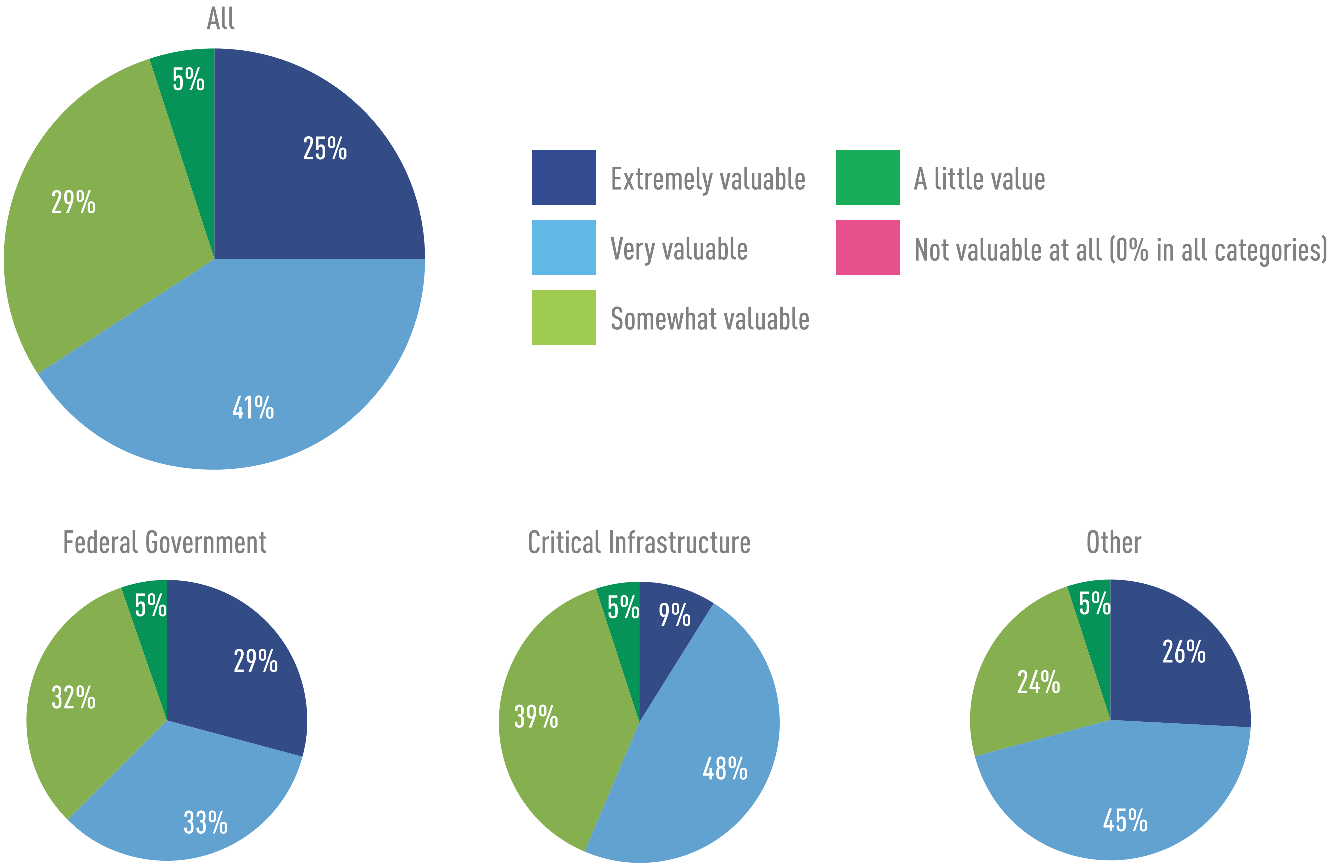
HALF OF NON-GOVERNMENTAL ORGANIZATIONS HAVE NOT FULLY ADOPTED NIST STANDARDS

Does your organization follow NIST standards for cybersecurity?



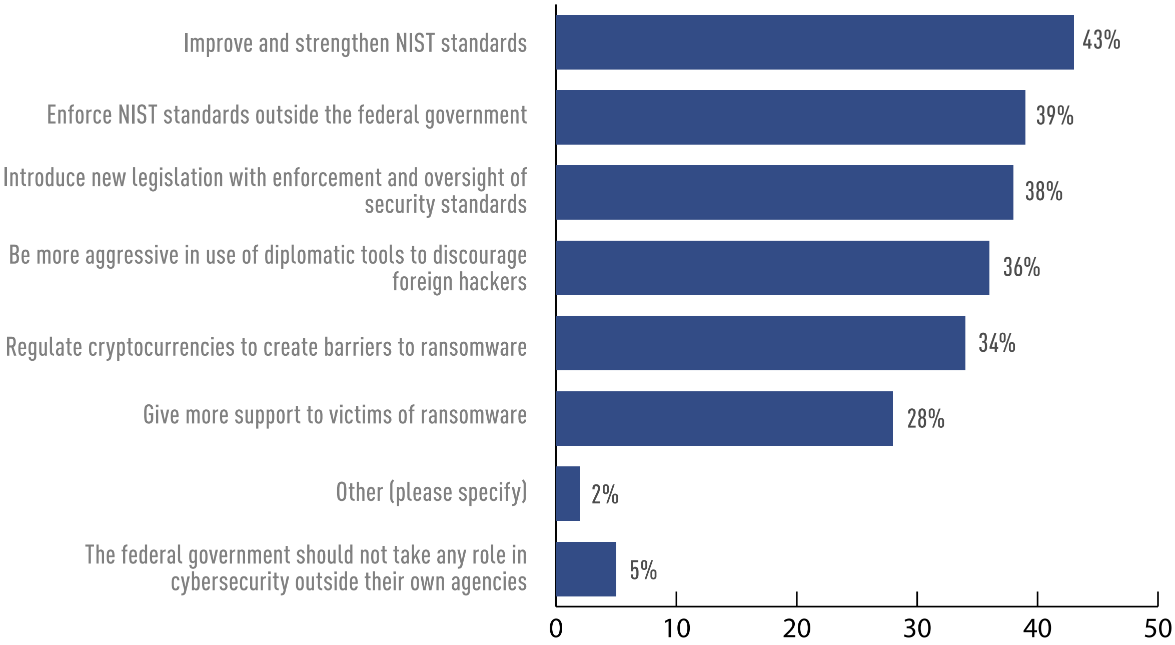
ALL FIND AT LEAST SOME VALUE IN NIST GUIDELINES, REGARDLESS OF LEVEL OF ADOPTION

What is your personal opinion of the value of the NIST guidelines for cybersecurity outcomes?



95% BELIEVE THAT THE GOVERNMENT SHOULD PLAY A BIGGER ROLE IN SECURING NON-GOVERNMENTAL ORGANIZATIONS

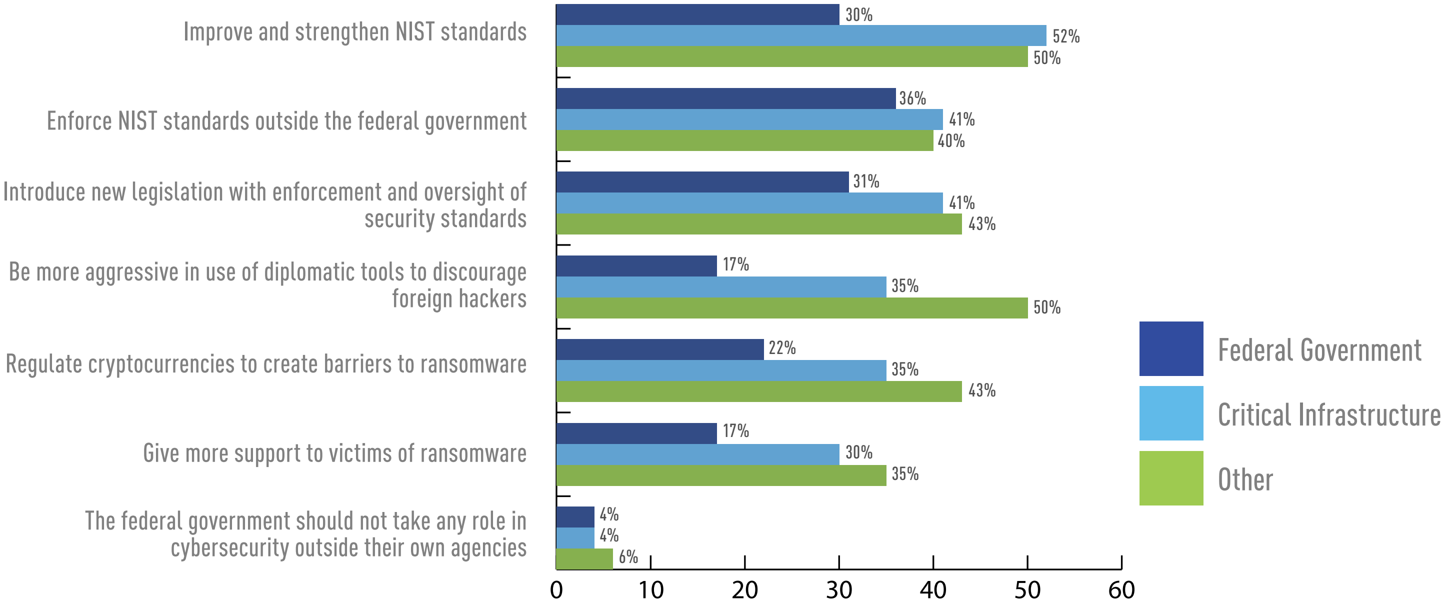
In your opinion, what additional efforts should the federal government take in ensuring the security of data and systems of *non-governmental* organizations? Choose all that apply.



Other: Most frequent replies: Make NIST easier to understand; Hold technology vendors accountable

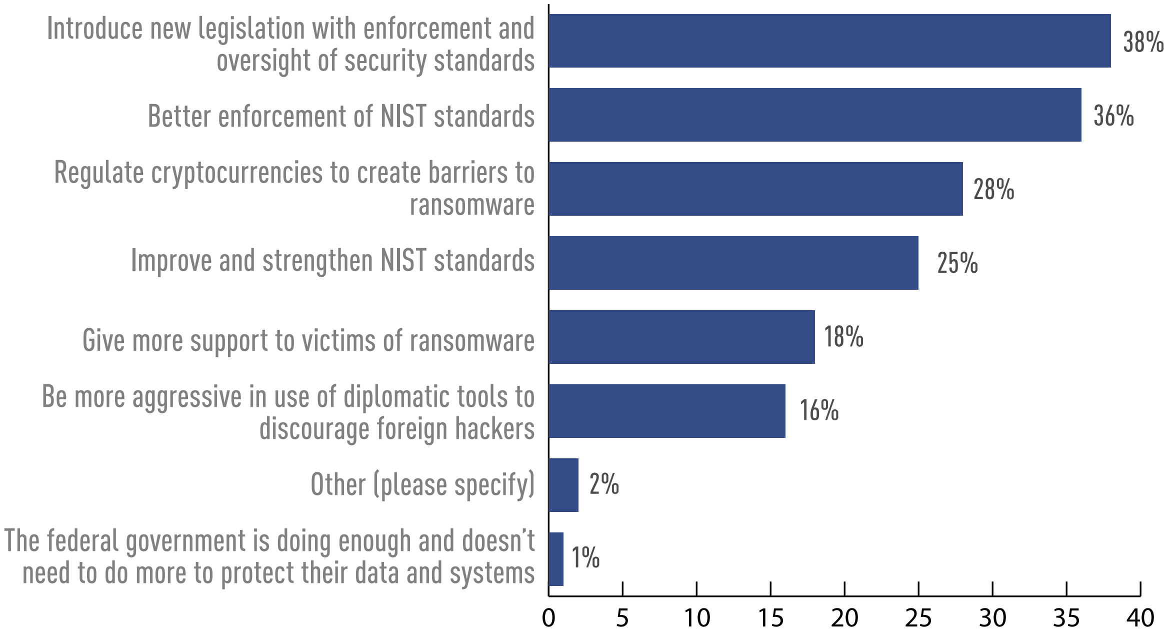
CRITICAL INFRASTRUCTURE IS SEEKING IMPROVEMENT AND ENFORCEMENT OF SECURITY STANDARDS, INCLUDING NIST GUIDELINES, FROM THE FED

In your opinion, what additional efforts should the federal government take in ensuring the security of data and systems of *non-governmental* organizations? Choose all that apply.



99% OF FEDERAL SECURITY PROS THINK THE GOVERNMENT SHOULD DO MORE TO PROTECT THEIR OWN DATA & SYSTEMS, INCLUDING BETTER ENFORCEMENT OF NIST STANDARDS

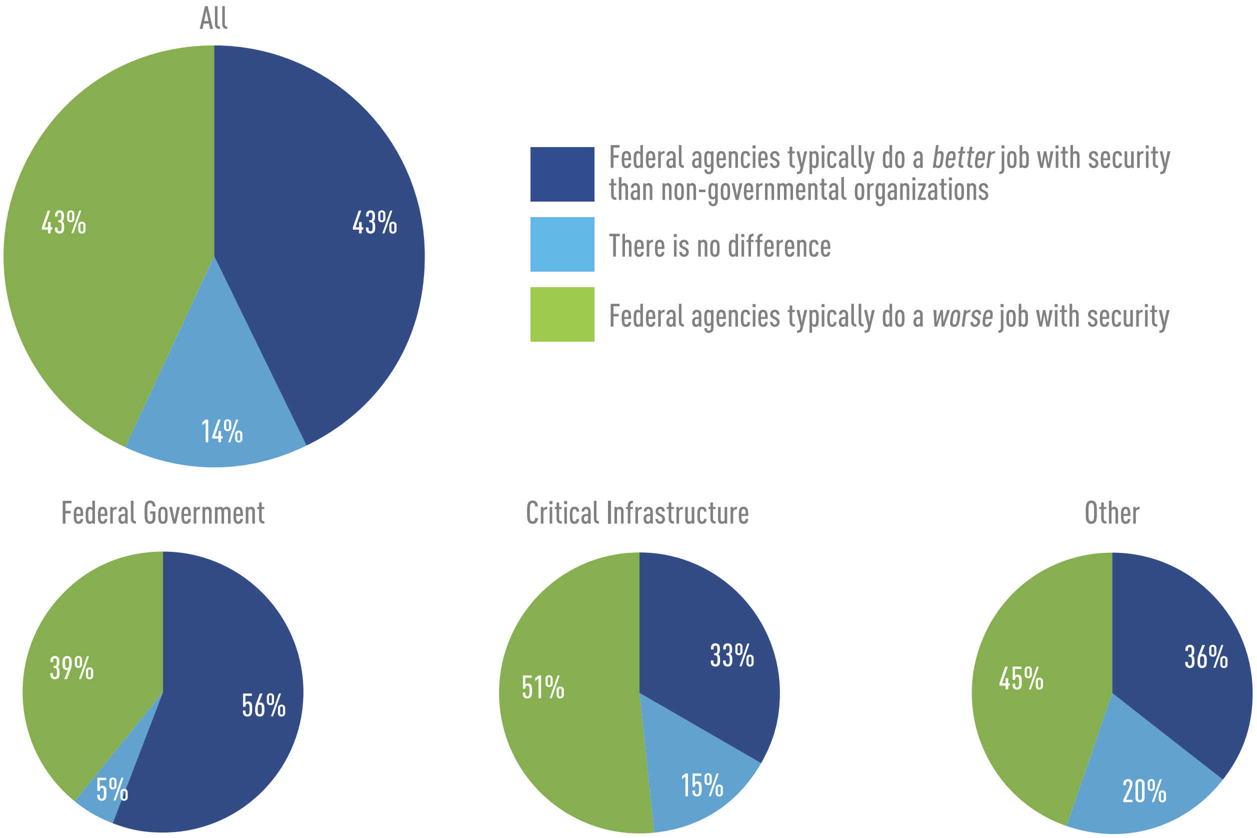
In your opinion, what additional efforts should the federal government take in ensuring the security of *government* data and systems? Choose all that apply.



Other: Proper staffing; rehire the guy that actually knew what he was doing

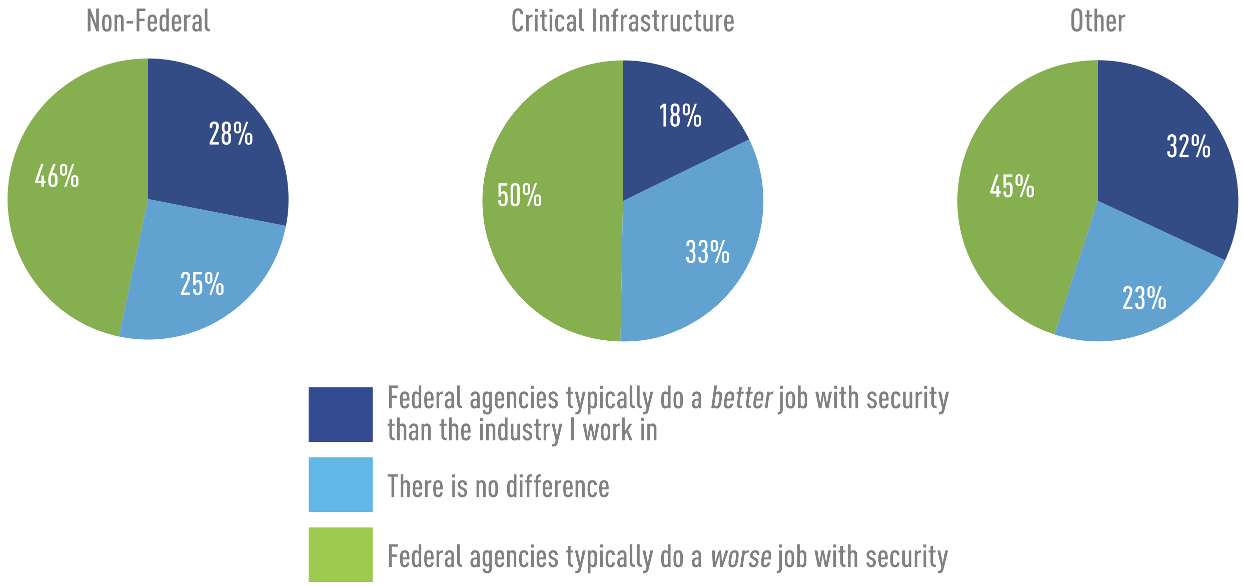
FEDERAL SECURITY PROFESSIONALS BELIEVE GOVERNMENT SYSTEMS ARE MORE SECURE THAN OTHER INDUSTRIES

In your opinion, how does the security of federal government data and systems compare to the cybersecurity efforts and outcomes of non-governmental organizations?



ON THE FLIP SIDE, *INDUSTRY* SECURITY PROS TYPICALLY THINK THE FEDERAL GOVERNMENT DOES A WORSE JOB WITH SECURITY

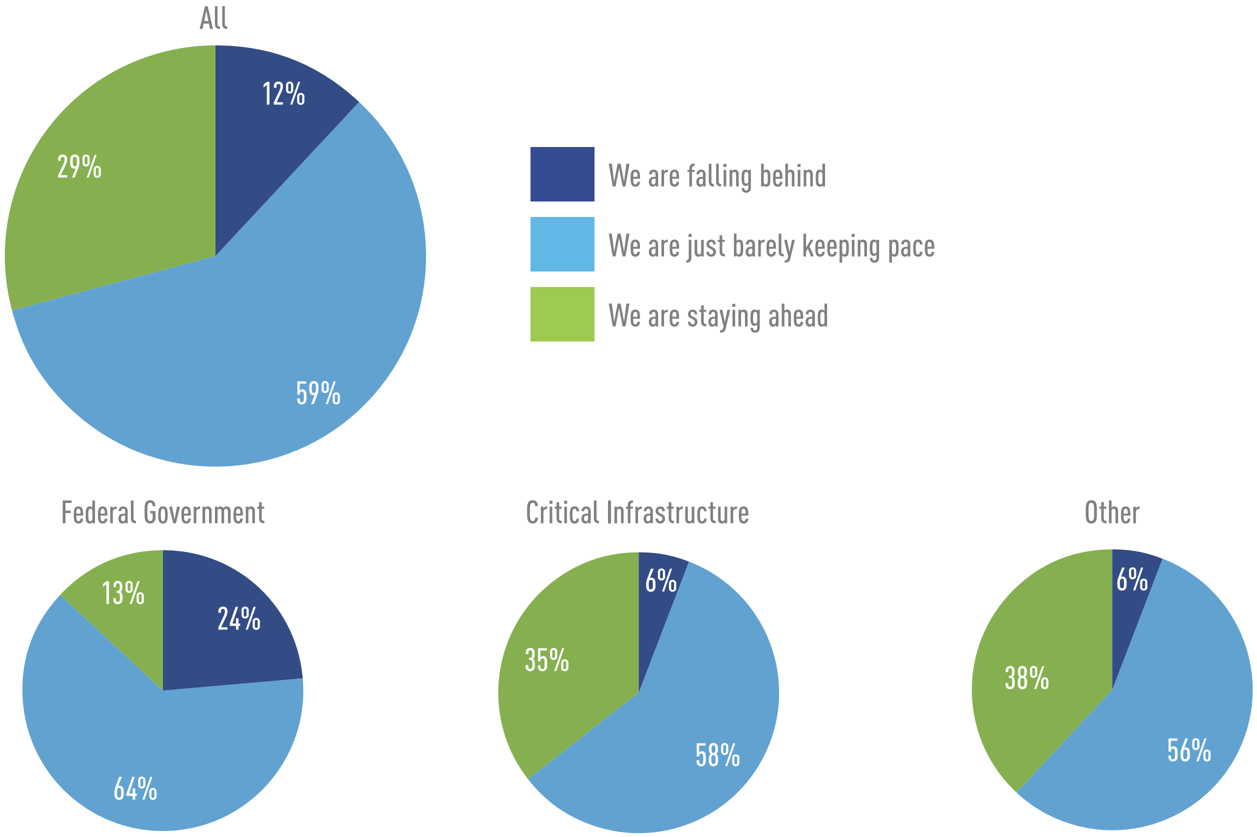
In your opinion, how does the security of federal government data and systems compare to compare to *your* industry's cybersecurity efforts and outcomes?



NEARLY A QUARTER OF FEDERAL SECURITY PROFESSIONALS FEEL THEY ARE FALLING BEHIND WHEN IT COMES TO PREPAREDNESS

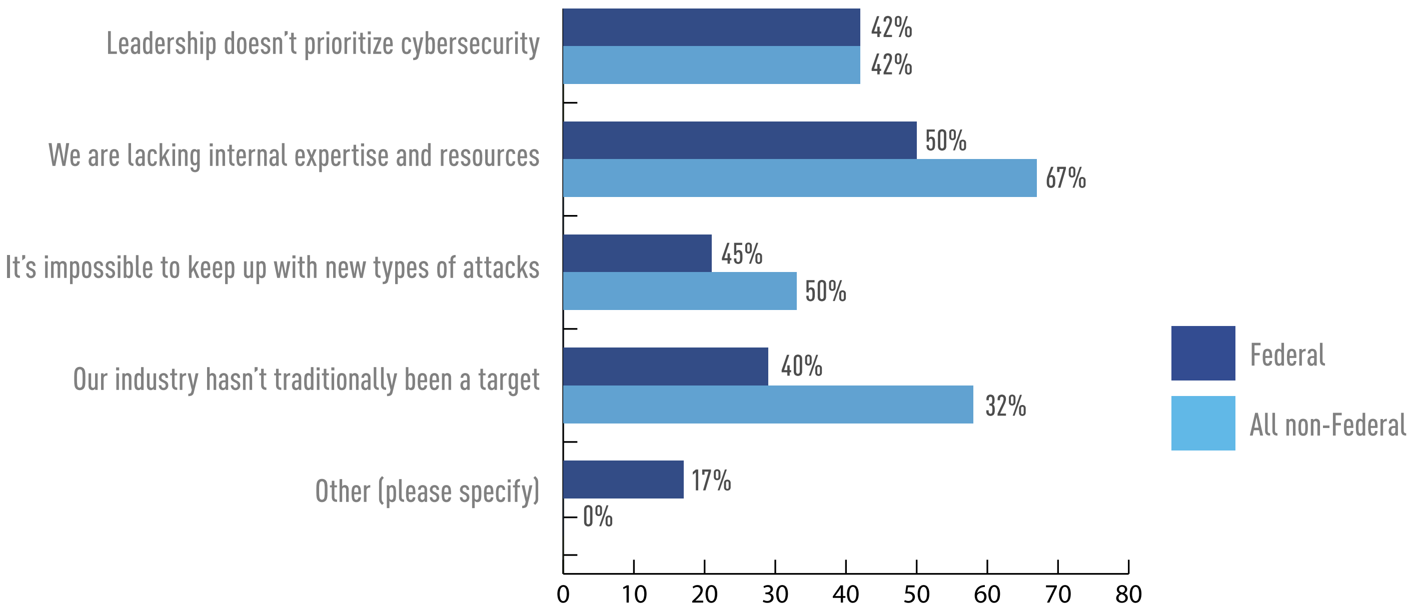
In your opinion, how prepared is your organization to face new threats and breaches?

Choose the one answer that most closely applies.



WIDE RANGE OF REASONS GIVEN FOR FALLING BEHIND WITH CYBERSECURITY EFFORTS

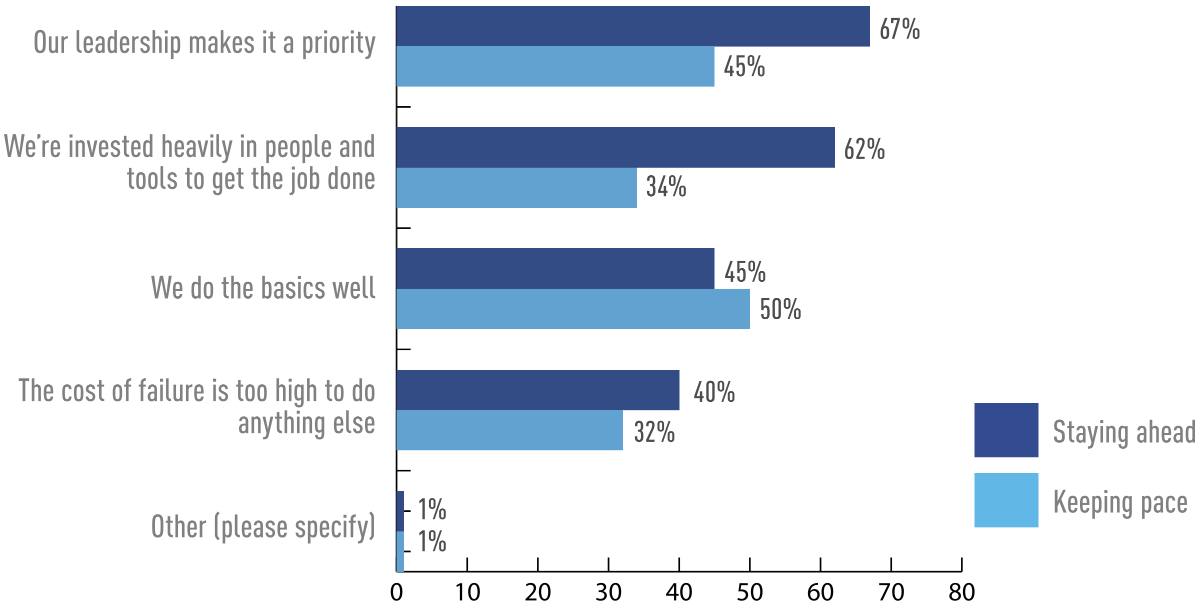
Why do you feel your organization is falling behind with cybersecurity efforts?



Other: Over reliance on "stand alone" network security; Staffing positions not backfilled

THE DIFFERENCE BETWEEN KEEPING PACE AND STAYING AHEAD IS LEADERSHIP AND INVESTMENT

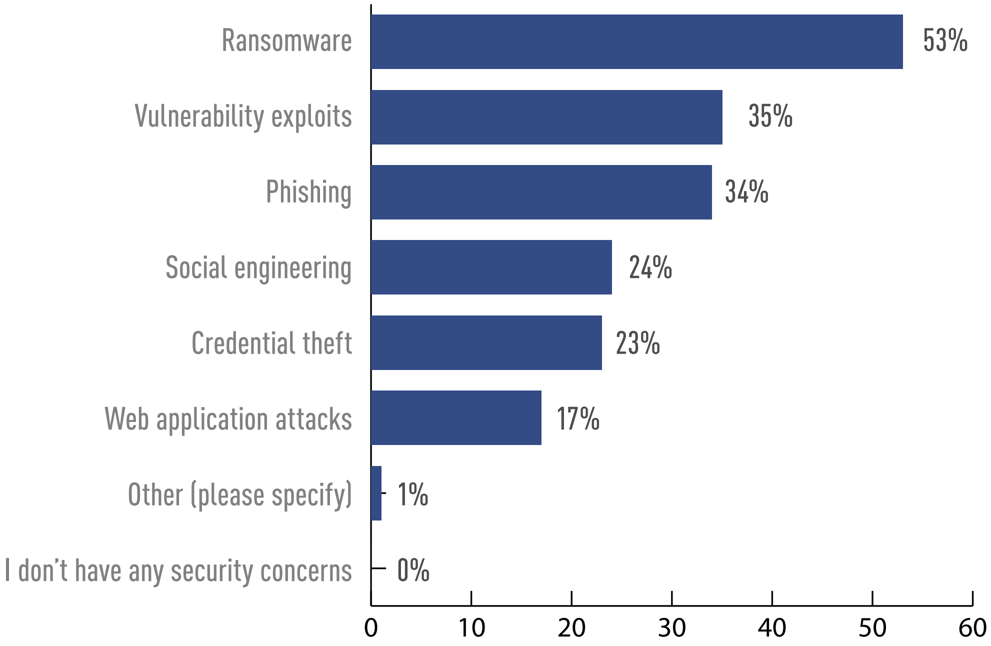
Why do you feel your organization is keeping pace or staying ahead with your cybersecurity efforts? Choose all that apply.



Other: We got burned by a ransomware attack which had convinced senior mgmt that they need to put $$$ into security; We are learning

RANSOMWARE TOPS LIST OF SECURITY CONCERNS

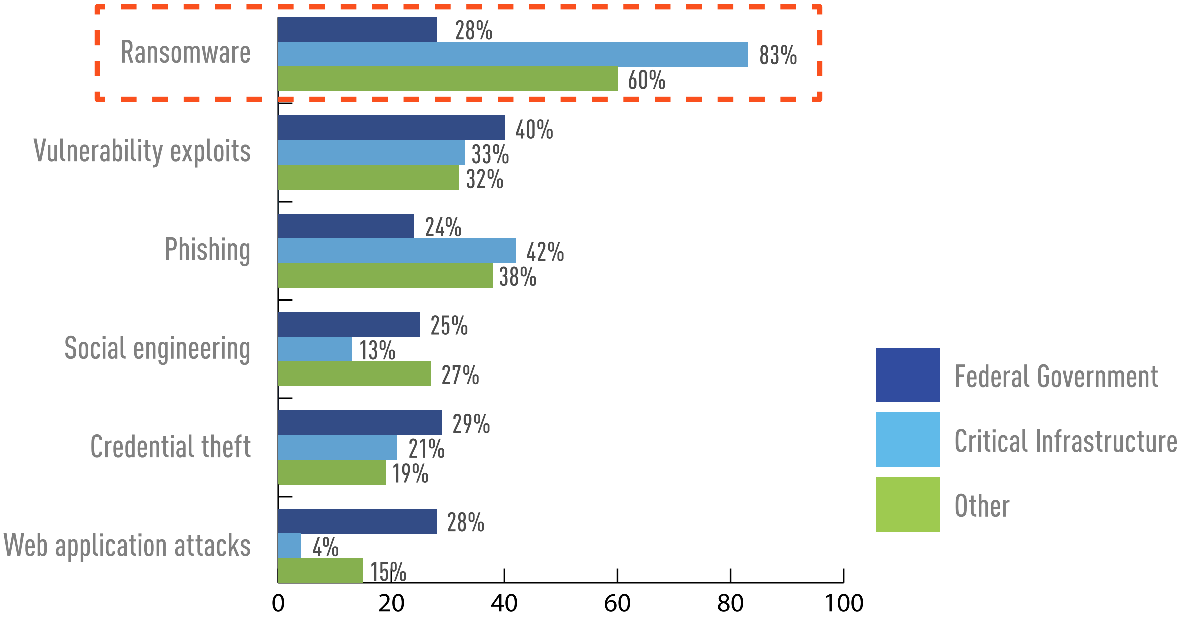
Which of the following types of security attacks are you *most* concerned about? Choose up to two of the following.



Other: DDoS; Office 365 attacks

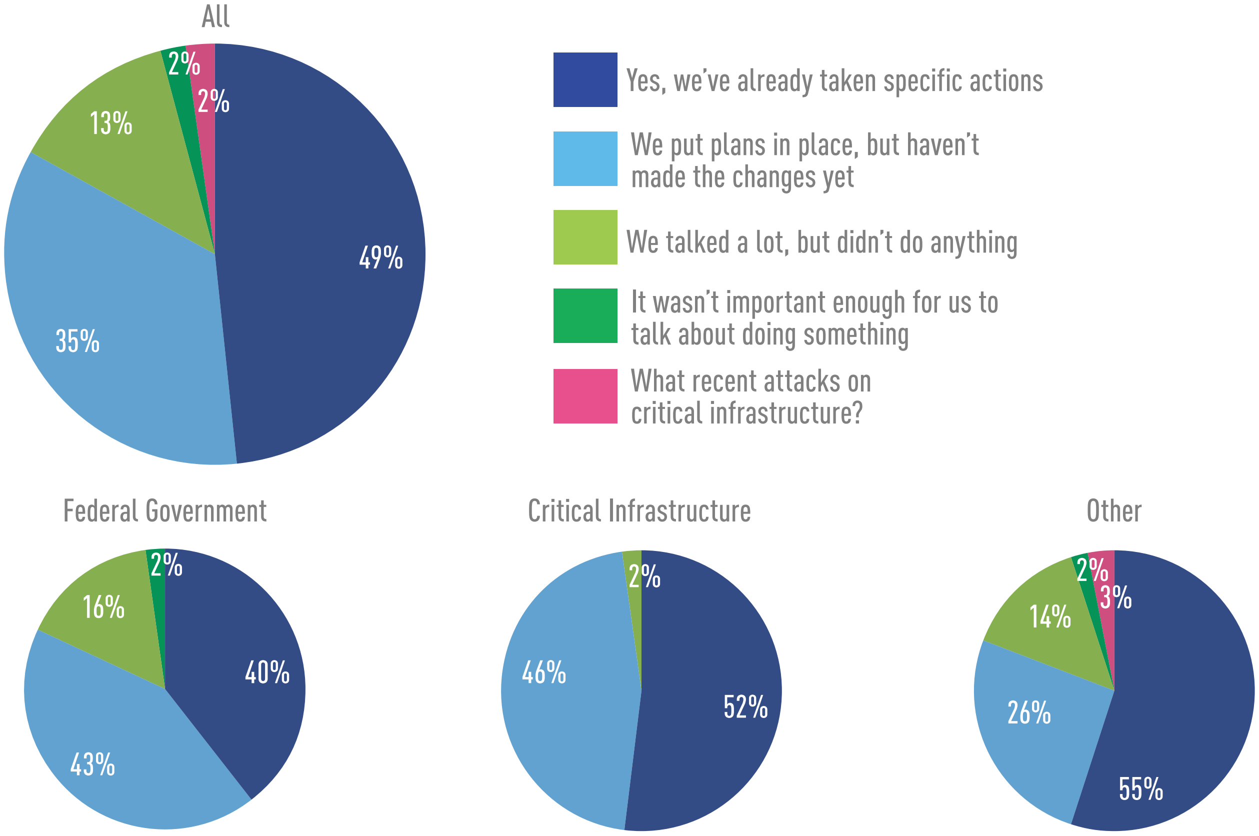
CRITICAL INFRASTRUCTURE IS MORE CONCERNED ABOUT RANSOMWARE THAN FEDERAL AGENCIES

Which of the following types of security attacks are you *most* concerned about?
Choose up to two of the following.



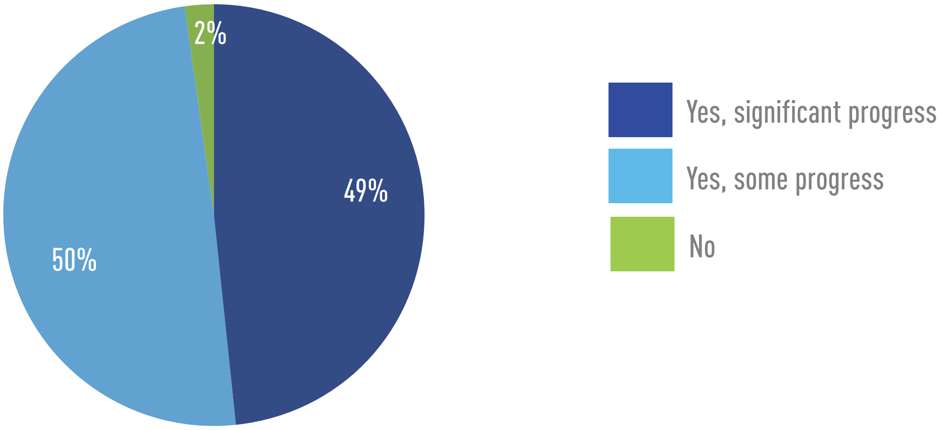
NON-FEDERAL ORGANIZATIONS TOOK GREATER ACTION IN LIGHT OF RECENT ATTACKS

Has your organization made any changes to your cybersecurity efforts as a result of recent attacks on critical infrastructure? Choose the one answer that most closely applies.



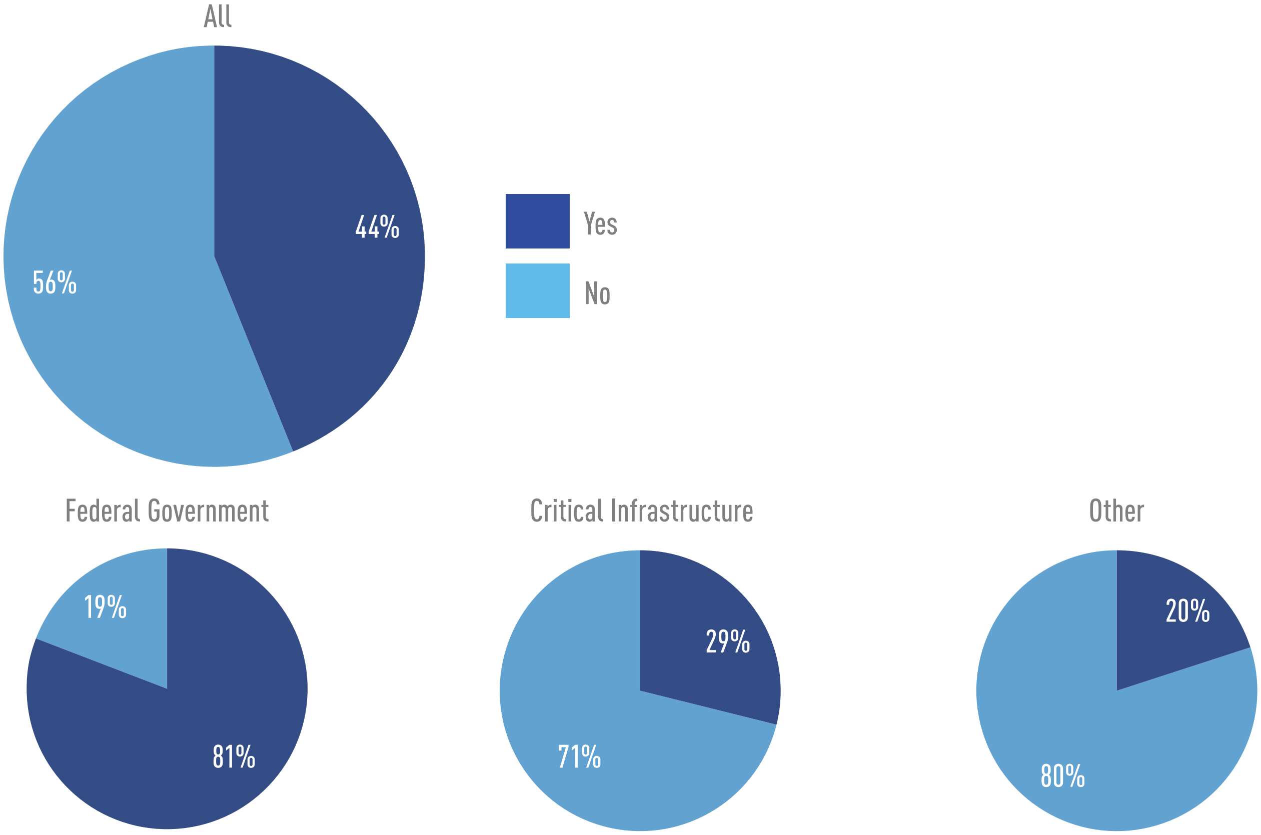
98% OF FED AGENCIES HAVE MADE AT LEAST SOME PROGRESS ON EXECUTIVE ORDERS ON CYBERSECURITY, NEARLY HALF NOTE SIGNIFICANT PROGRESS

Has your agency made progress in meeting the requirements of the executive order on cybersecurity?



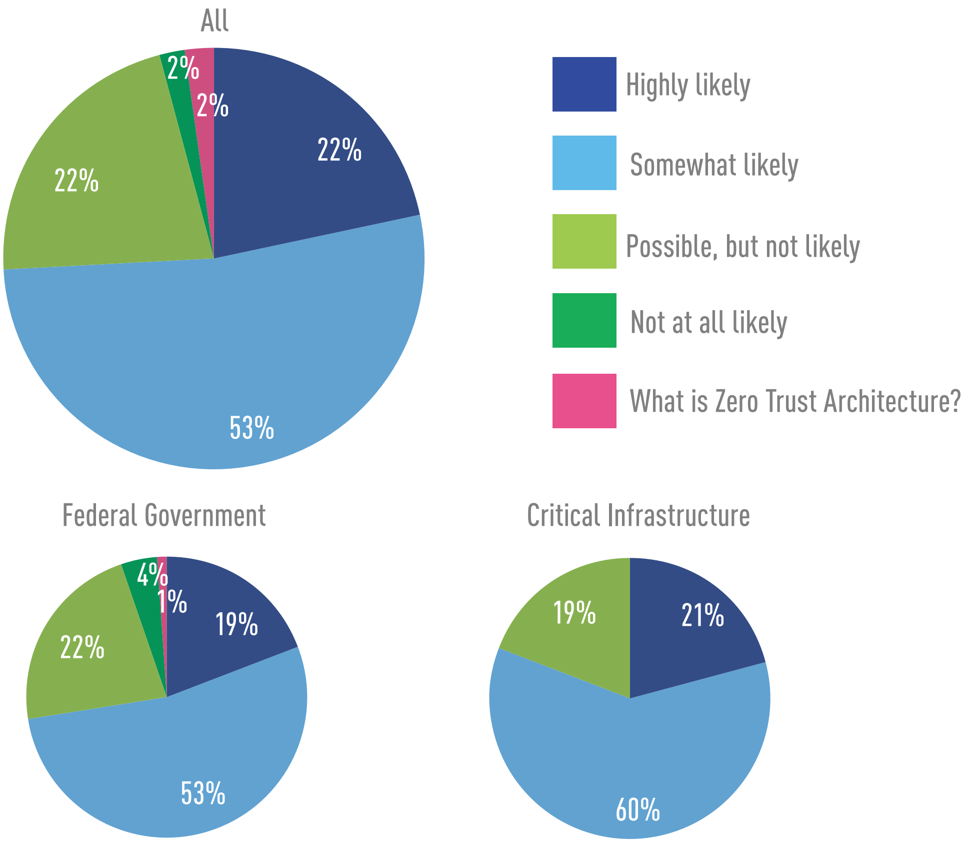
FEDERAL SECURITY PROS DISAGREE WITH OTHER INDUSTRIES ON GOVERNMENT RANSOMWARE EFFORTS

In your opinion, is the federal government doing enough to prevent ransomware attacks?



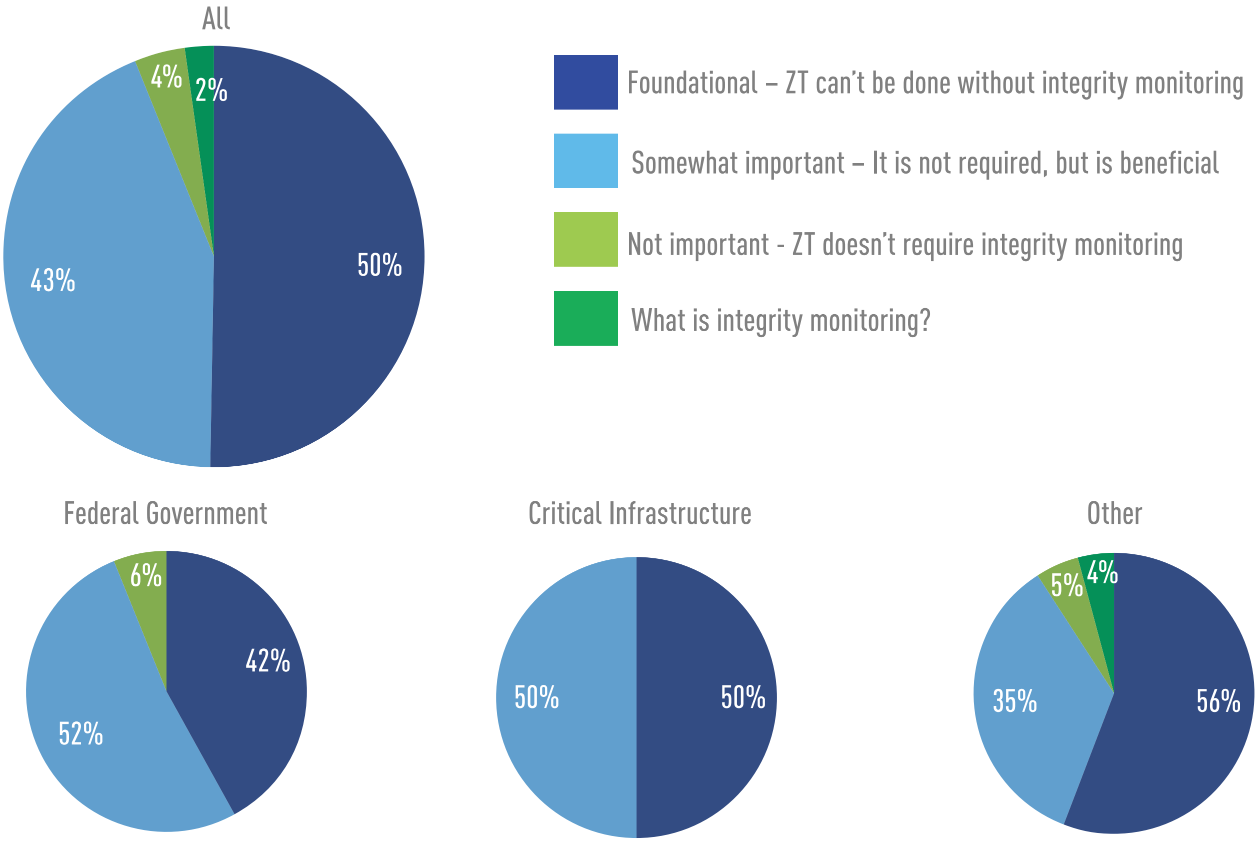
ALL INDUSTRIES IN AGREEMENT THAT ZERO TRUST WILL IMPROVE SECURITY OUTCOMES

In your opinion, how likely is it that Zero Trust Architecture (ZTA) will materially improve cybersecurity outcomes?



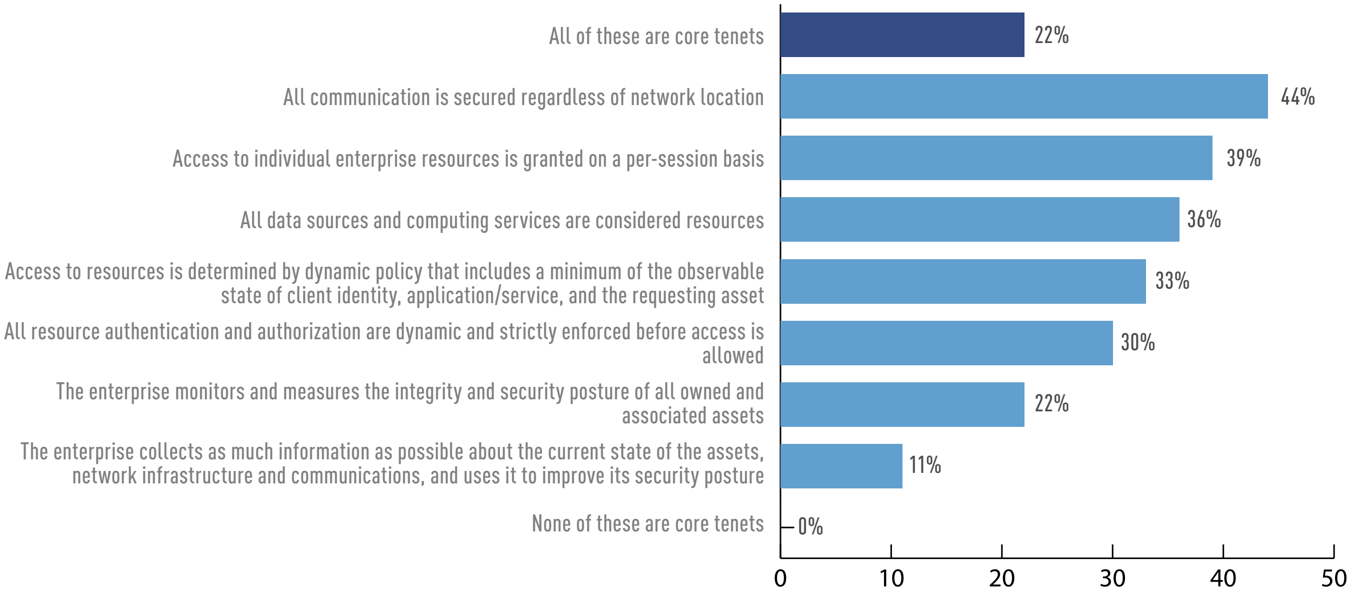
ALMOST ALL BELIEVE INTEGRITY MONITORING IS IMPORTANT TO ZERO TRUST

In your experience, how important is integrity monitoring to a successful Zero Trust (ZT) strategy?



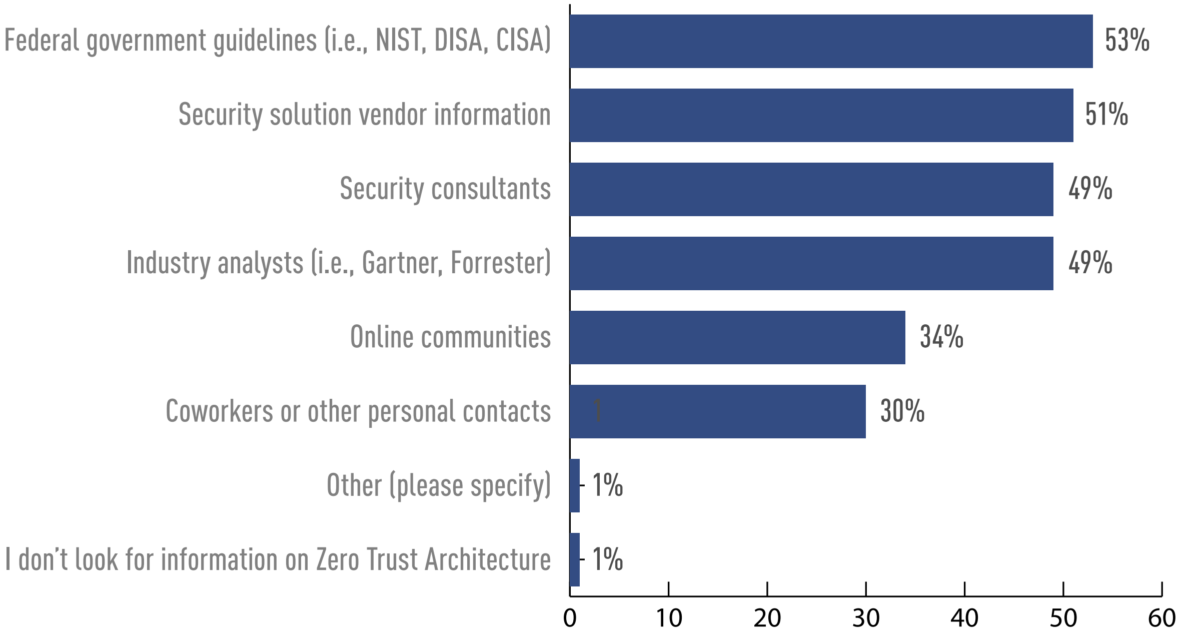
THOSE FAMILIAR WITH ZERO TRUST MOST COMMONLY IDENTIFIED SECURE COMMUNICATION AND LIMITING INDIVIDUAL ACCESS AS CORE TENETS

Which of the following do you consider to be core tenets of Zero Trust? Choose all that apply.



FEDERAL GOVERNMENT GUIDELINES THE TOP SOURCE OF ZERO TRUST INFORMATION

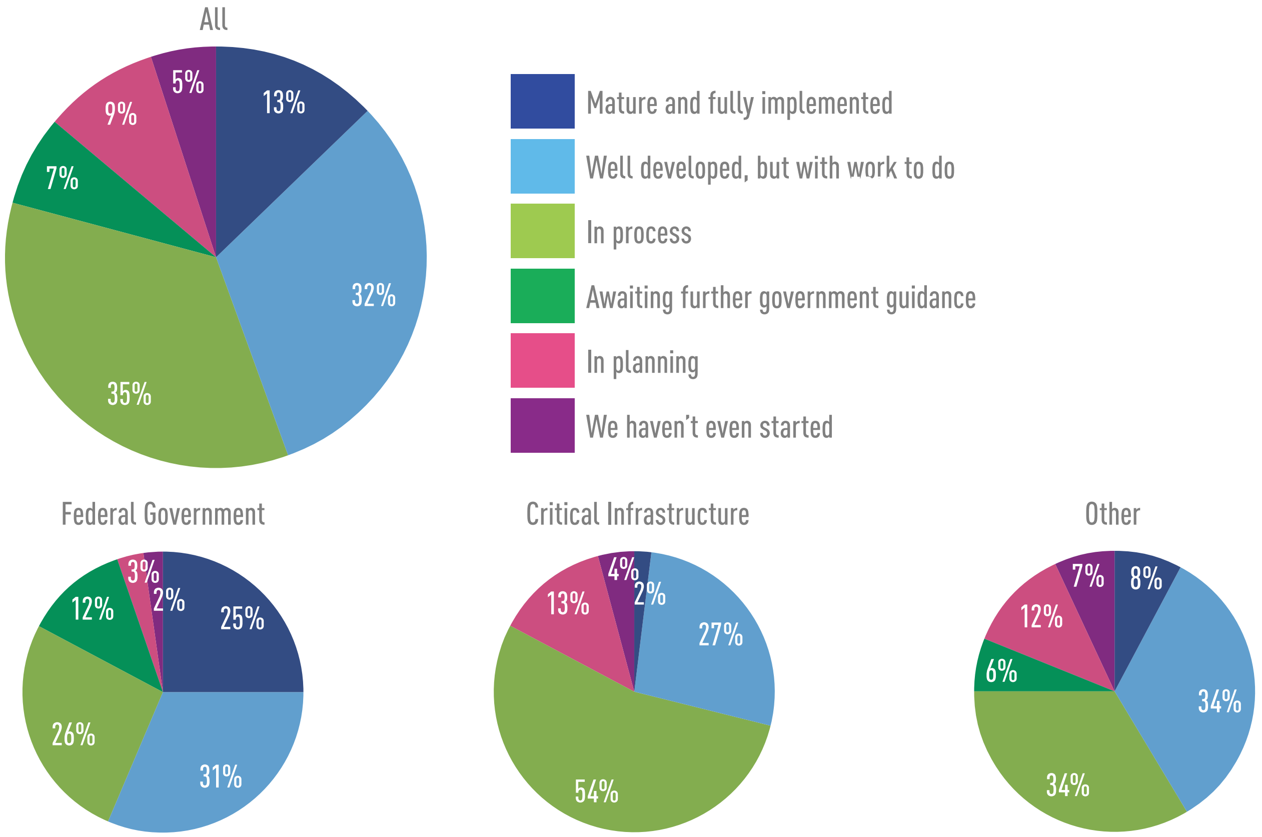
When you look for guidelines, best practices, or other information on Zero Trust Architecture strategies, what sources do you use? Choose all that apply.



Other: Industry associations; My own opinions on security

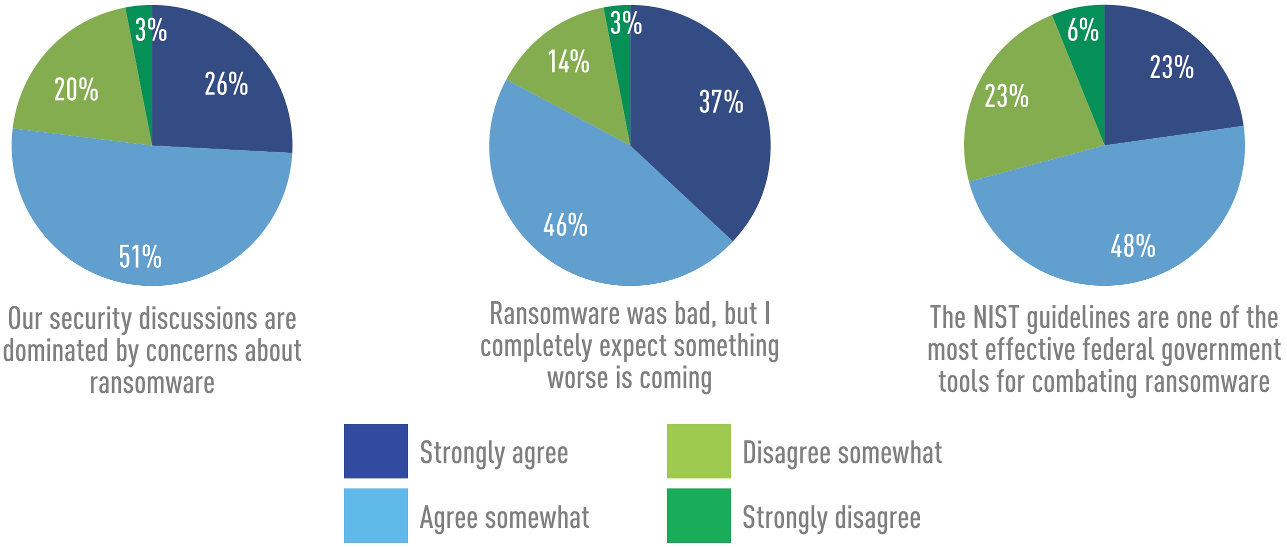
FEDERAL GOVERNMENT REPORTS SLIGHTLY BETTER PROGRESS TOWARD ZERO TRUST ADOPTION

How would you describe your company's progress towards Zero Trust adoption?
Choose the one answer that most closely applies.



83% EXPECT SOMETHING WORSE THAN RANSOMWARE IS GOING TO HIT THE SECURITY WORLD

Please indicate your agreement with each of the following statements.



Our security discussions are dominated by concerns about ransomware

Ransomware was bad, but I completely expect something worse is coming

The NIST guidelines are one of the most effective federal government tools for combating ransomware

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook