Midterm Group Project

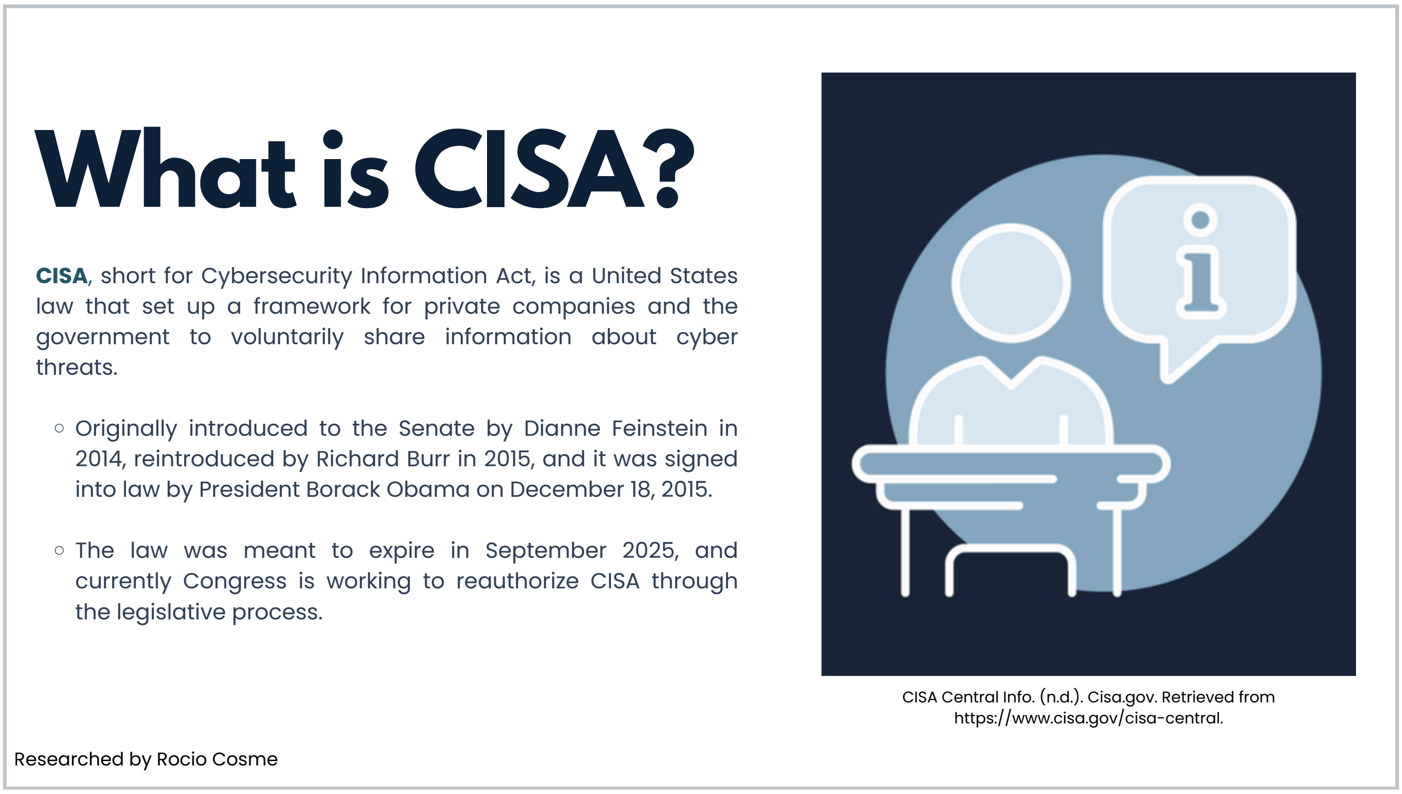
Understanding CISA

CISA. (n.d.-a). Cisa Logo. Retrieved from https://www.cisa.gov/topics/election-security/election-security-training.

1.7.2013

Title page: The Policy our group chose to work on is CISA, and we will be covering the many components of the law as well as how it can be improved in the end.

‹#›



What is CISA?

CISA, short for Cybersecurity Information Act, is a United States law that set up a framework for private companies and the government to voluntarily share information about cyber threats.

- Originally introduced to the Senate by Dianne Feinstein in 2014, reintroduced by Richard Burr in 2015, and it was signed into law by President Borack Obama on December 18, 2015.
- The law was meant to expire in September 2025, and currently Congress is working to reauthorize CISA through the legislative process.

CISA Central Info. (n.d.). Cisa.gov. Retrieved from https://www.cisa.gov/cisa-central.

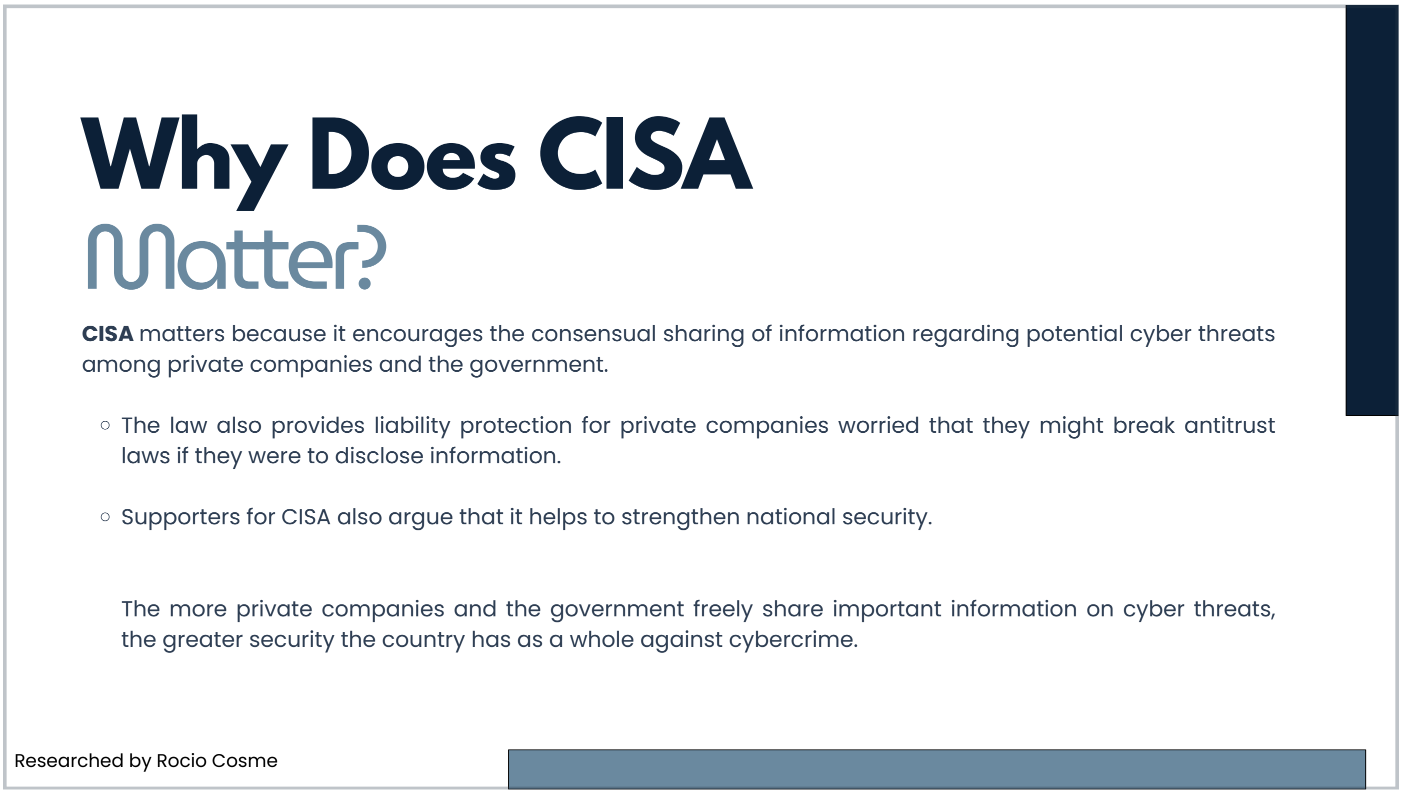
Researched by Rocio Cosme

1.7.2013

CISA, or the Cybersecurity Information Sharing Act, was created to let private companies and the government share cyber threat data more easily.

The law is set to expire in 2025, and Congress is now working to reauthorize it to keep improving national cybersecurity collaboration.

‹#›



Why Does CISA Matter?

CISA matters because it encourages the consensual sharing of information regarding potential cyber threats among private companies and the government.

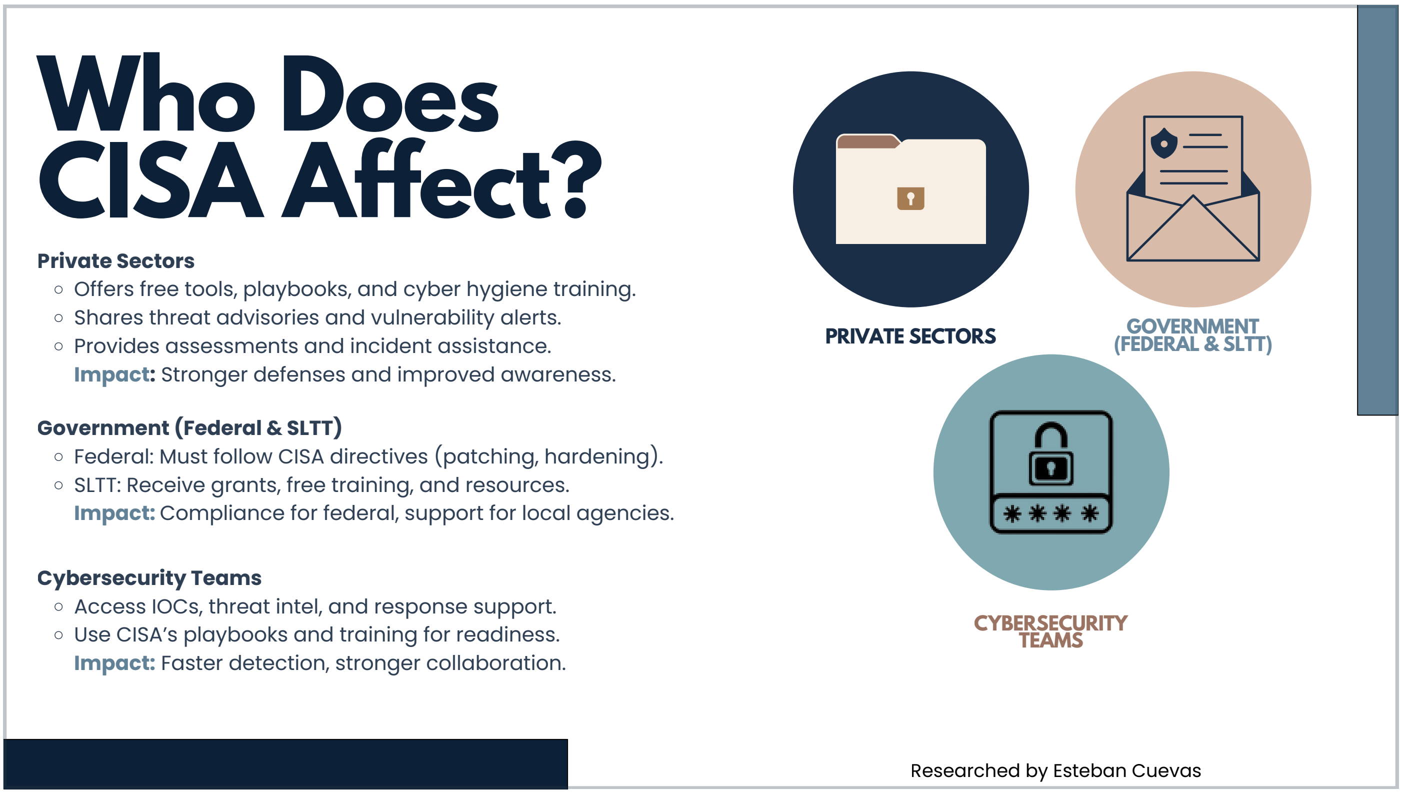
- The law also provides liability protection for private companies worried that they might break antitrust laws if they were to disclose information.
- Supporters for CISA also argue that it helps to strengthen national security.

The more private companies and the government freely share important information on cyber threats, the greater security the country has as a whole against cybercrime.

Researched by Rocio Cosme

1.7.2013

CISA’s work has made the U.S. more resilient against major cyberattacks and inspired international cooperation.



Who Does CISA Affect?

Private Sectors

- Offers free tools, playbooks, and cyber hygiene training.
- Shares threat advisories and vulnerability alerts.
- Provides assessments and incident assistance.

Impact: Stronger defenses and improved awareness.

Government (Federal & SLTT)

- Federal: Must follow CISA directives (patching, hardening).
- SLTT: Receive grants, free training, and resources.

Impact: Compliance for federal, support for local agencies.

Cybersecurity Teams

- Access IOCs, threat intel, and response support.
- Use CISA's playbooks and training for readiness.

Impact: Faster detection, stronger collaboration.

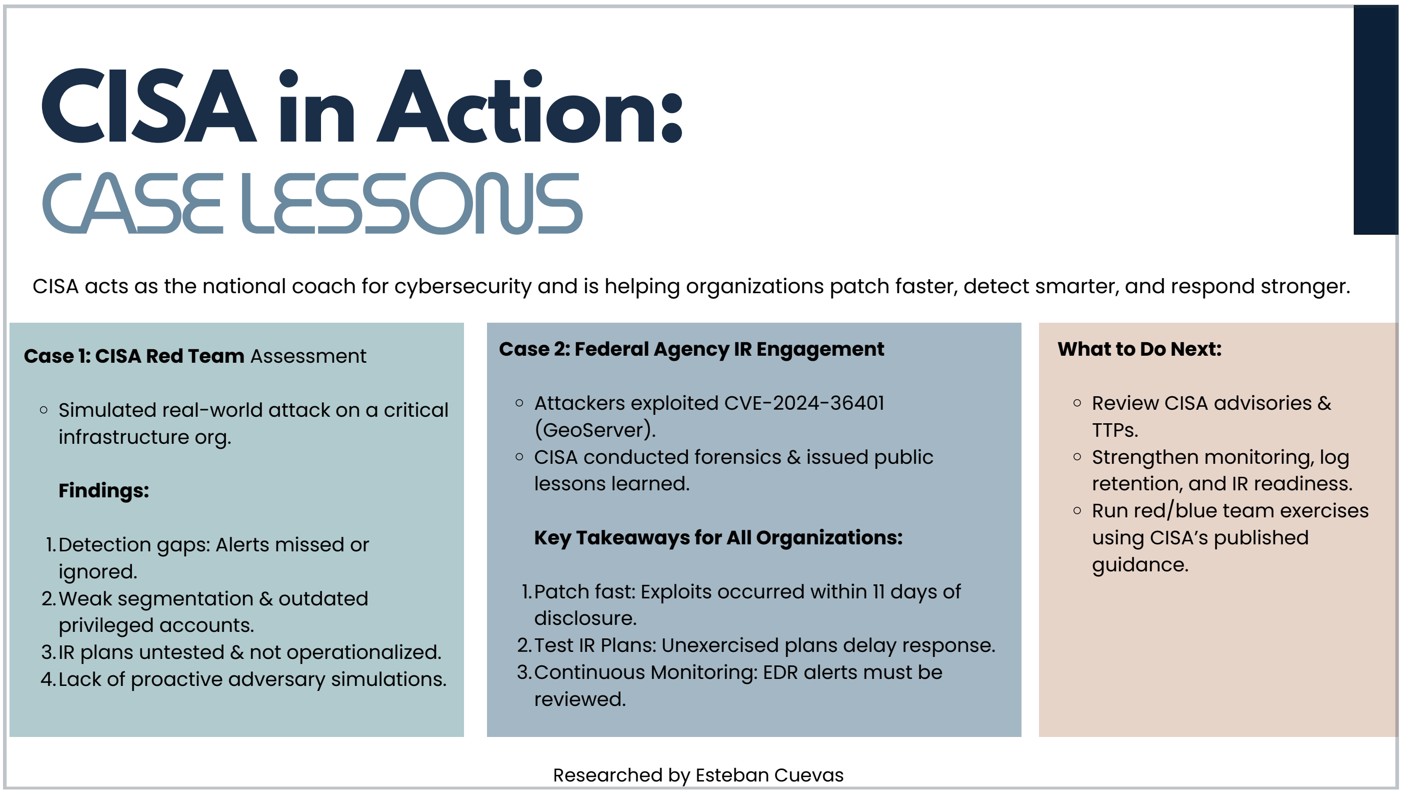
Researched by Esteban Cuevas

1.7.2013

CISA supports private sectors with free tools, training.
The government must follow CISA directives, while state and local entities get grants and training support.

Cybersecurity teams also benefit from access to threat intelligence and response tools, improving collaboration and detection speed across sectors

‹#›



CISA in Action:
CASE LESSONS

CISA acts as the national coach for cybersecurity and is helping organizations patch faster, detect smarter, and respond stronger.

Case 1: CISA Red Team Assessment

- Simulated real-world attack on a critical infrastructure org.

Findings:

1. Detection gaps: Alerts missed or ignored.
2. Weak segmentation & outdated privileged accounts.
3. IR plans untested & not operationalized.
4. Lack of proactive adversary simulations.

Case 2: Federal Agency IR Engagement

- Attackers exploited CVE-2024-36401 (GeoServer).
- CISA conducted forensics & issued public lessons learned.

Key Takeaways for All Organizations:

1. Patch fast: Exploits occurred within 11 days of disclosure.
2. Test IR Plans: Unexercised plans delay response.
3. Continuous Monitoring: EDR alerts must be reviewed.

What to Do Next:

- Review CISA advisories & TTPs.
- Strengthen monitoring, log retention, and IR readiness.
- Run red/blue team exercises using CISA's published guidance.

Researched by Esteban Cuevas

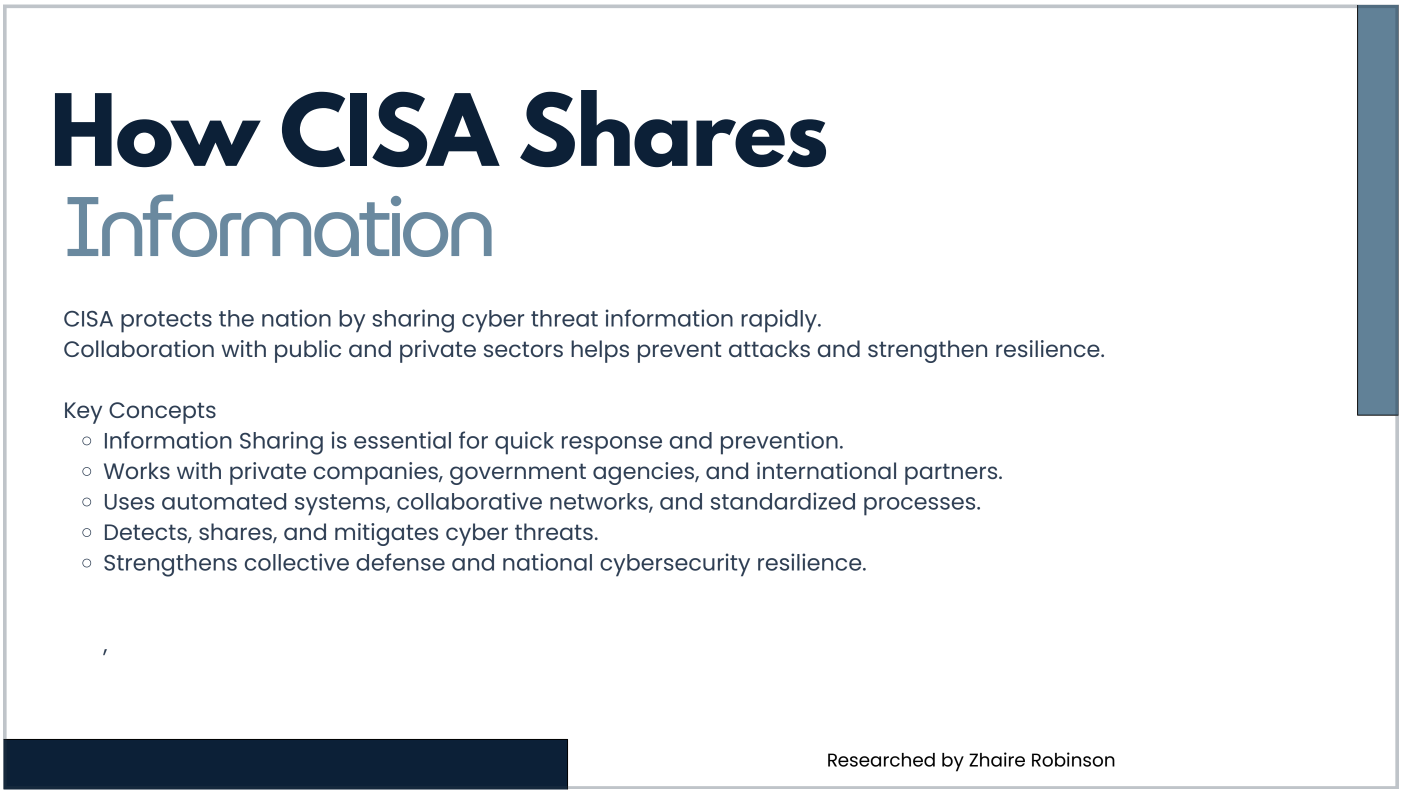
1.7.2013

CISA acts like a national cybersecurity coach, helping organizations detect, patch, and respond better.

The first case showed detection gaps and weak incident readiness in a critical infrastructure organization.

The second involved a real exploit that CISA helped contain and shared lessons learned publicly.

‹#›



How CISA Shares Information

CISA protects the nation by sharing cyber threat information rapidly.
Collaboration with public and private sectors helps prevent attacks and strengthen resilience.

Key Concepts

- Information Sharing is essential for quick response and prevention.
- Works with private companies, government agencies, and international partners.
- Uses automated systems, collaborative networks, and standardized processes.
- Detects, shares, and mitigates cyber threats.
- Strengthens collective defense and national cybersecurity resilience.

,

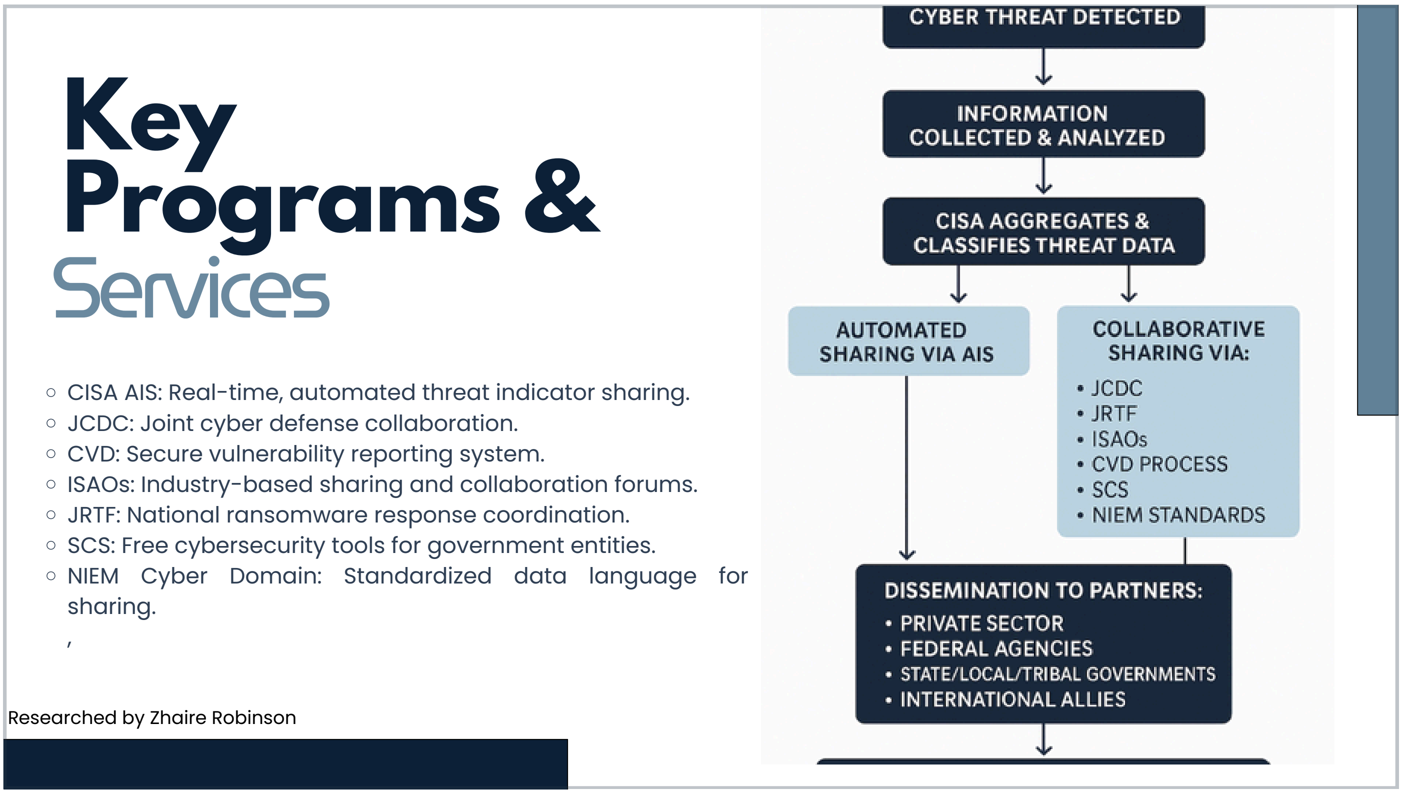
Researched by Zhaire Robinson

1.7.2013

CISA shares cyber threat information to prevent and reduce attacks.

It works with private companies, government agencies, and international partners. Real-time sharing builds stronger national cybersecurity and collective defense.

‹#›



Key Programs & Services

- CISA AIS: Real-time, automated threat indicator sharing.
- JCDC: Joint cyber defense collaboration.
- CVD: Secure vulnerability reporting system.
- ISAOs: Industry-based sharing and collaboration forums.
- JRTF: National ransomware response coordination.
- SCS: Free cybersecurity tools for government entities.
- NIEM Cyber Domain: Standardized data language for sharing.

,

Researched by Zhaire Robinson

CYBER THREAT DETECTED

INFORMATION COLLECTED & ANALYZED

CISA AGGREGATES & CLASSIFIES THREAT DATA

AUTOMATED SHARING VIA AIS

COLLABORATIVE SHARING VIA:

- JCDC
- JRTF
- ISAOs
- CVD PROCESS
- SCS
- NIEM STANDARDS

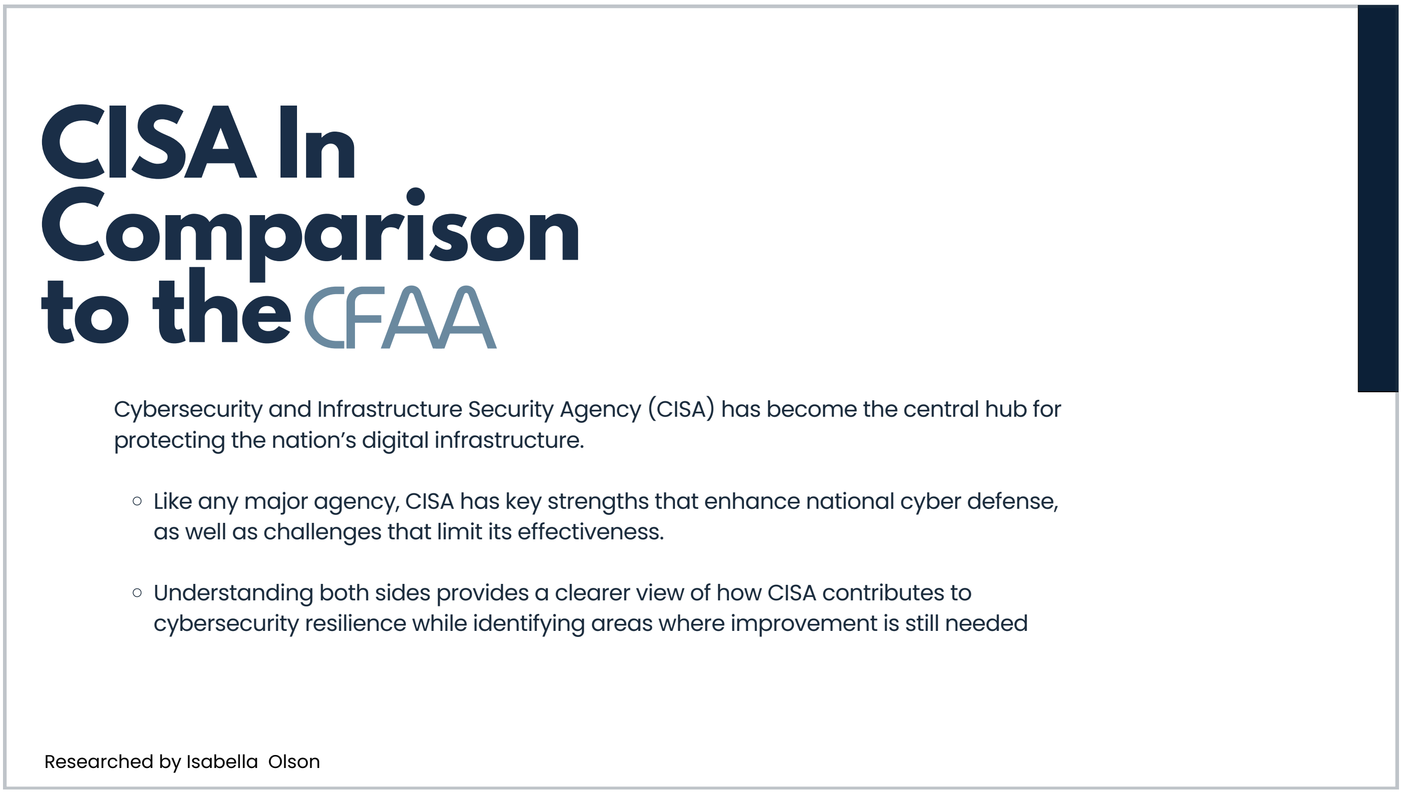
DISSEMINATION TO PARTNERS:

- PRIVATE SECTOR
- FEDERAL AGENCIES
- STATE/LOCAL/TRIBAL GOVERNMENTS
- INTERNATIONAL ALLIES

1.7.2013

This slide highlights CISA’s key programs and services for cybersecurity information sharing. CISA collects and analyzes threat data, then classifies it to ensure partners receive accurate, actionable intelligence.
The chart visually shows how information gets shared

‹#›



CISA In Comparison to the CFAA

Cybersecurity and Infrastructure Security Agency (CISA) has become the central hub for protecting the nation’s digital infrastructure.

- Like any major agency, CISA has key strengths that enhance national cyber defense, as well as challenges that limit its effectiveness.
- Understanding both sides provides a clearer view of how CISA contributes to cybersecurity resilience while identifying areas where improvement is still needed

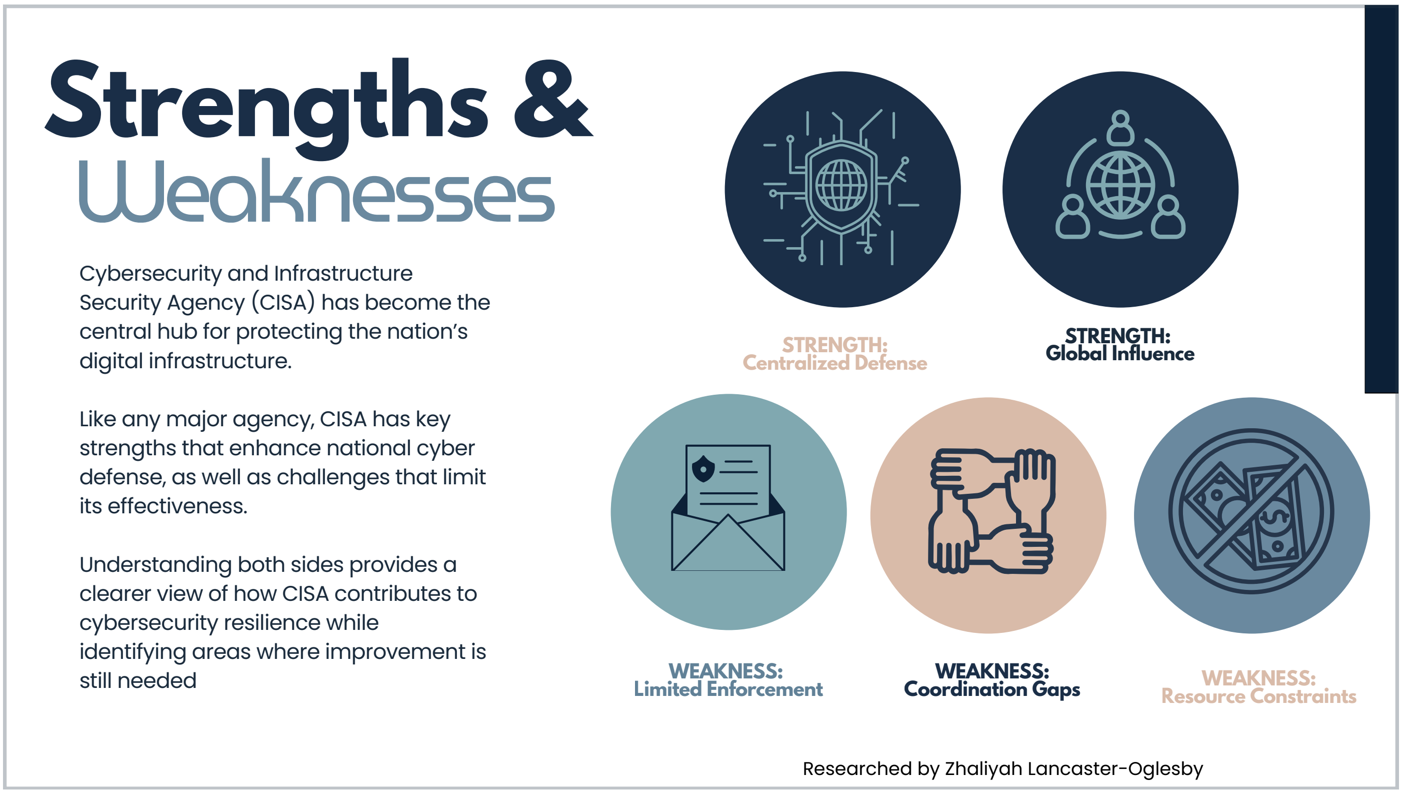
Researched by Isabella Olson

1.7.2013

On this slide, I’m comparing the Cybersecurity and Infrastructure Security Agency, or CISA, with the Computer Fraud and Abuse Act, or CFA
CISA is a federal agency created in 2018 under the Department of Homeland Security. Its main goal is to protect the nation’s critical infrastructure things like energy grids, hospitals, transportation systems, and government networks.

They focus on prevention, coordination, and resilience- working with both public and private sectors to respond to and reduce cyber risks.

‹#›



Strengths & Weaknesses

Cybersecurity and Infrastructure Security Agency (CISA) has become the central hub for protecting the nation’s digital infrastructure.

Like any major agency, CISA has key strengths that enhance national cyber defense, as well as challenges that limit its effectiveness.

Understanding both sides provides a clearer view of how CISA contributes to cybersecurity resilience while identifying areas where improvement is still needed

STRENGTH:
Centralized Defense

STRENGTH:
Global Influence

WEAKNESS:
Limited Enforcement

WEAKNESS:
Coordination Gaps

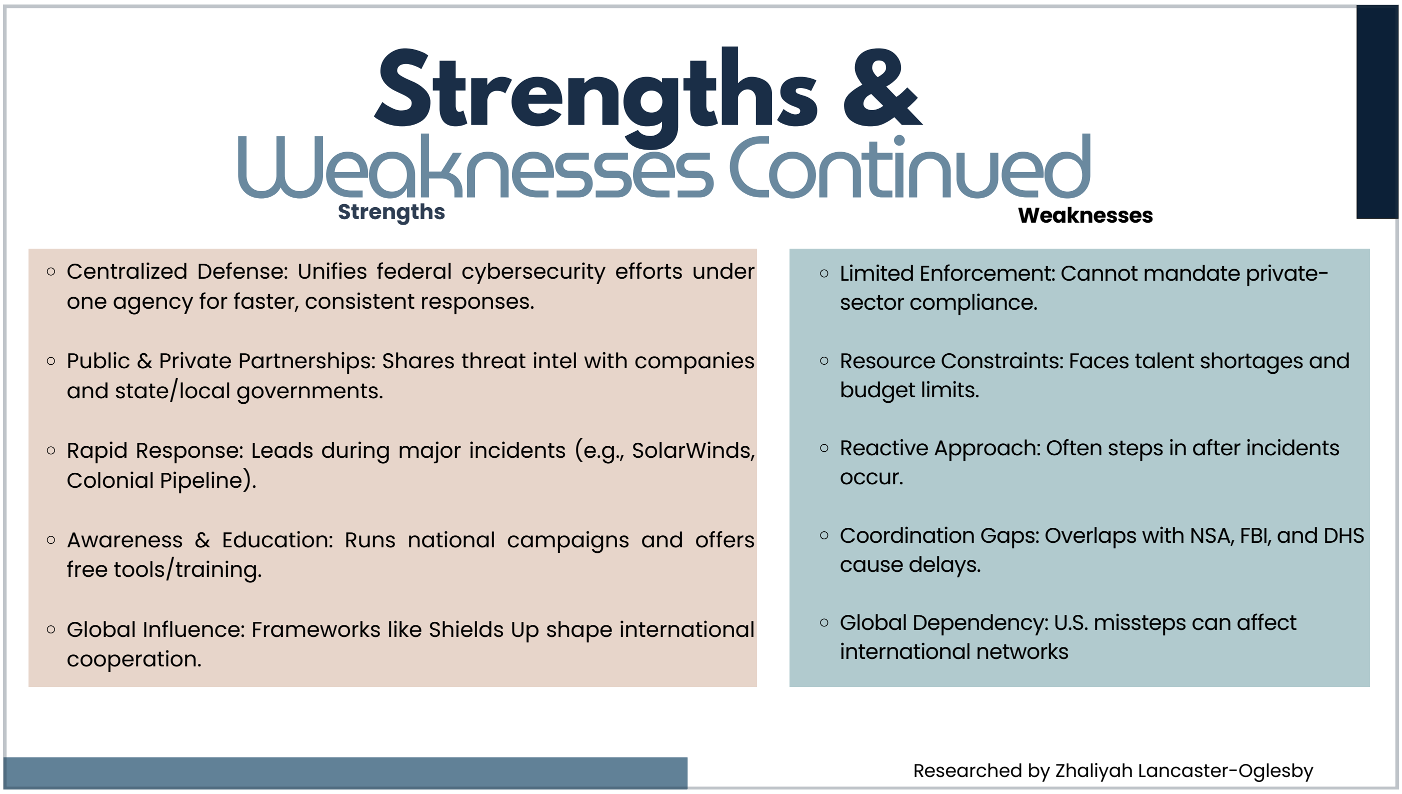
WEAKNESS:
Resource Constraints

Researched by Zhaliyah Lancaster-Oglesby

1.7.2013

This slide highlights CISA’s main strengths and weaknesses.
and explains why understanding both is key to having a clear view of how CISA works

‹#›



Strengths & Weaknesses Continued

Strengths

- Centralized Defense: Unifies federal cybersecurity efforts under one agency for faster, consistent responses.
- Public & Private Partnerships: Shares threat intel with companies and state/local governments.
- Rapid Response: Leads during major incidents (e.g., SolarWinds, Colonial Pipeline).
- Awareness & Education: Runs national campaigns and offers free tools/training.
- Global Influence: Frameworks like Shields Up shape international cooperation.

Weaknesses

- Limited Enforcement: Cannot mandate private-sector compliance.
- Resource Constraints: Faces talent shortages and budget limits.
- Reactive Approach: Often steps in after incidents occur.
- Coordination Gaps: Overlaps with NSA, FBI, and DHS cause delays.
- Global Dependency: U.S. missteps can affect international networks

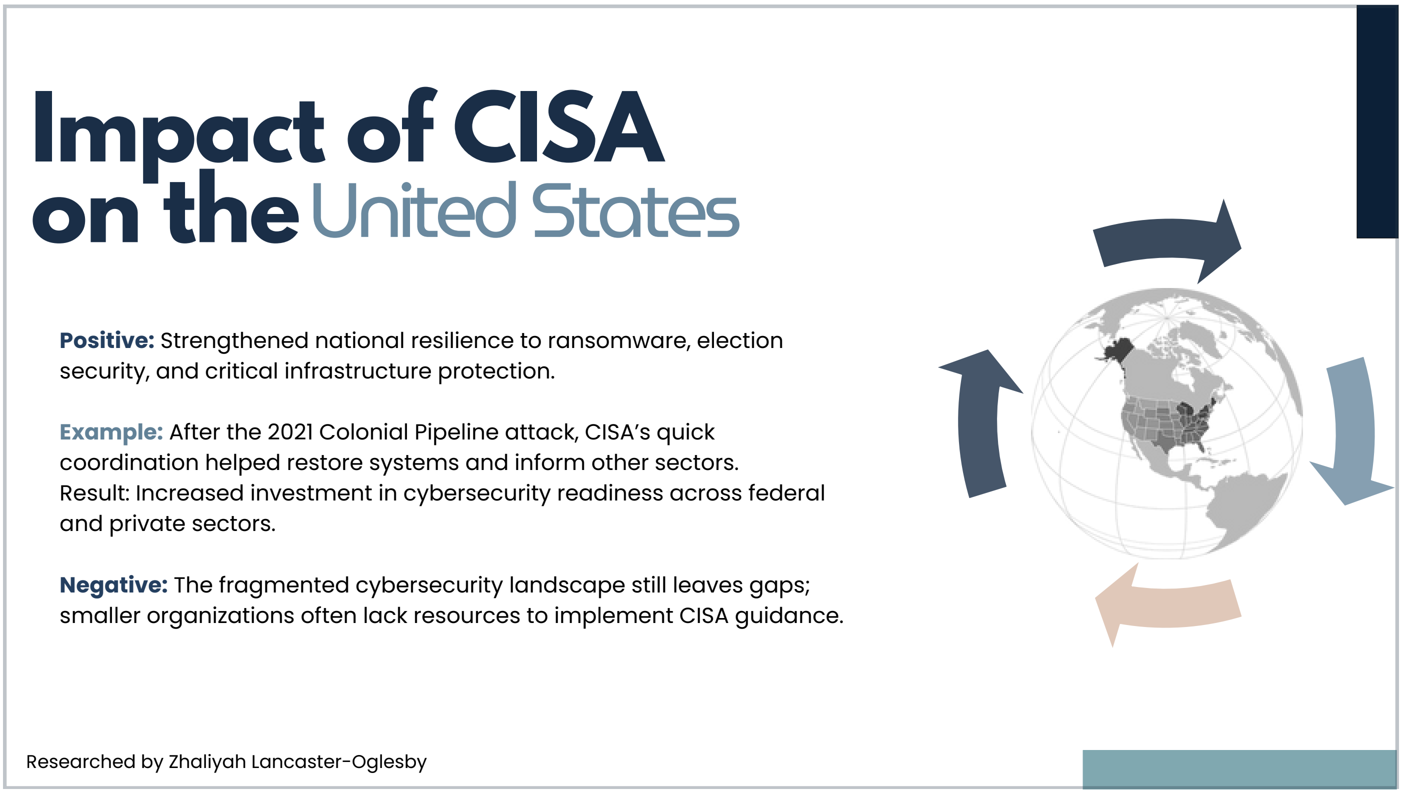
Researched by Zhaliyah Lancaster-Oglesby

1.7.2013

Covers the positive side of CISA, highlighting centralized U.S. cyber defense, strong public-private partnerships, and major incident responses.

CISA also has limits, like it can’t enforce compliance on private companies, struggles to keep talent, and sometimes reacts instead of preventing. Coordination challenges and global reliance on U.S. systems also create risks

‹#›



Impact of CISA on the United States

Positive: Strengthened national resilience to ransomware, election security, and critical infrastructure protection.

Example: After the 2021 Colonial Pipeline attack, CISA's quick coordination helped restore systems and inform other sectors.
Result: Increased investment in cybersecurity readiness across federal and private sectors.

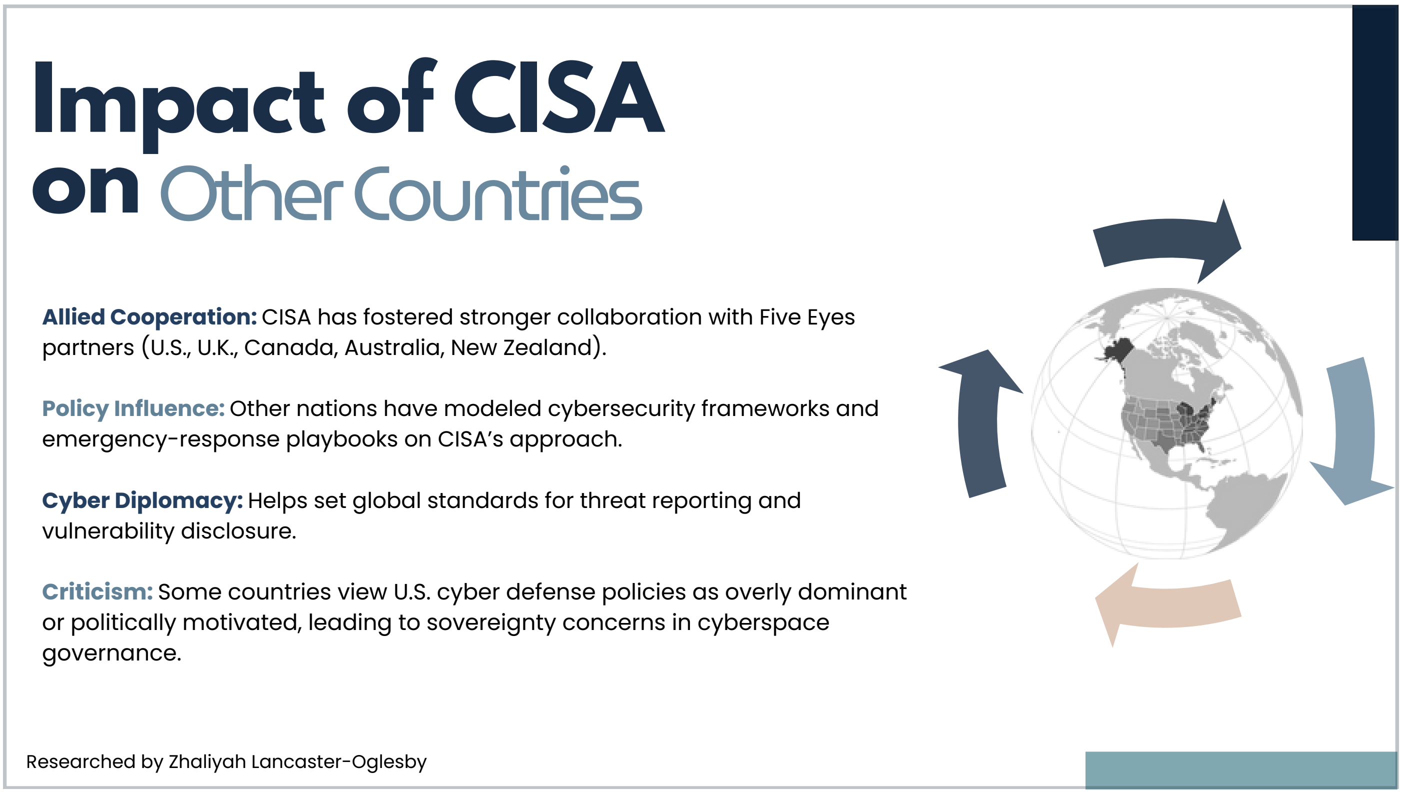
Negative: The fragmented cybersecurity landscape still leaves gaps; smaller organizations often lack resources to implement CISA guidance.

Researched by Zhaliyah Lancaster-Oglesby

1.7.2013

CISA has strengthened U.S. cybersecurity, improving resilience against ransomware, election threats, and attacks on critical infrastructure. While these efforts have boosted cybersecurity nationwide, gaps remain as smaller organizations struggle to implement CISA guidance fully.

‹#›



Impact of CISA on Other Countries

Allied Cooperation: CISA has fostered stronger collaboration with Five Eyes partners (U.S., U.K., Canada, Australia, New Zealand).

Policy Influence: Other nations have modeled cybersecurity frameworks and emergency-response playbooks on CISA's approach.

Cyber Diplomacy: Helps set global standards for threat reporting and vulnerability disclosure.

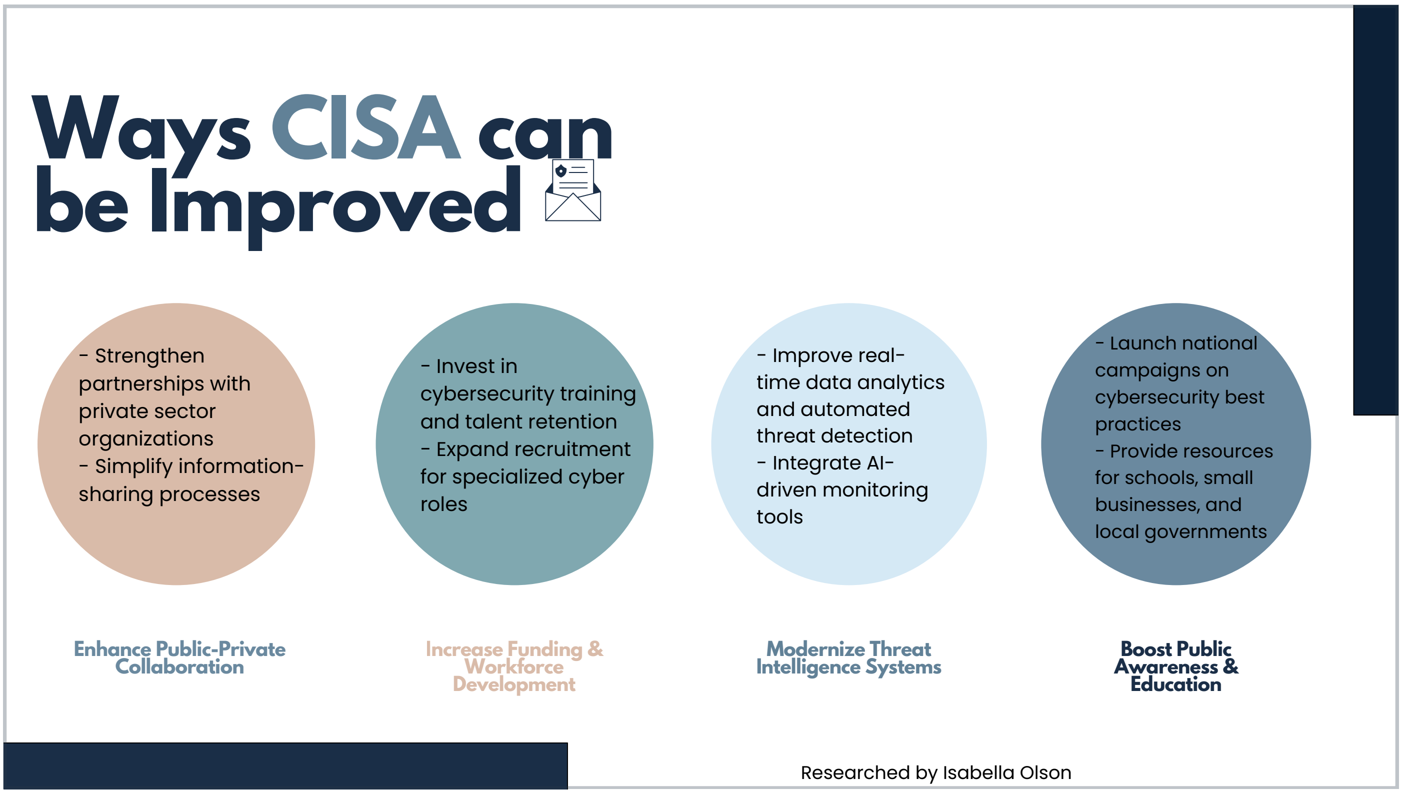
Criticism: Some countries view U.S. cyber defense policies as overly dominant or politically motivated, leading to sovereignty concerns in cyberspace governance.

Researched by Zhaliyah Lancaster-Oglesby

1.7.2013

Globally, CISA's frameworks influence allied cybersecurity strategies, though some countries worry about relying too much on U.S. control in cyberspace

‹#›



Ways CISA can be Improved

- Strengthen partnerships with private sector organizations
- Simplify information-sharing processes

Enhance Public-Private Collaboration

- Invest in cybersecurity training and talent retention
- Expand recruitment for specialized cyber roles

Increase Funding & Workforce Development

- Improve real-time data analytics and automated threat detection
- Integrate AI-driven monitoring tools

Modernize Threat Intelligence Systems

- Launch national campaigns on cybersecurity best practices
- Provide resources for schools, small businesses, and local governments

Boost Public Awareness & Education

Researched by Isabella Olson

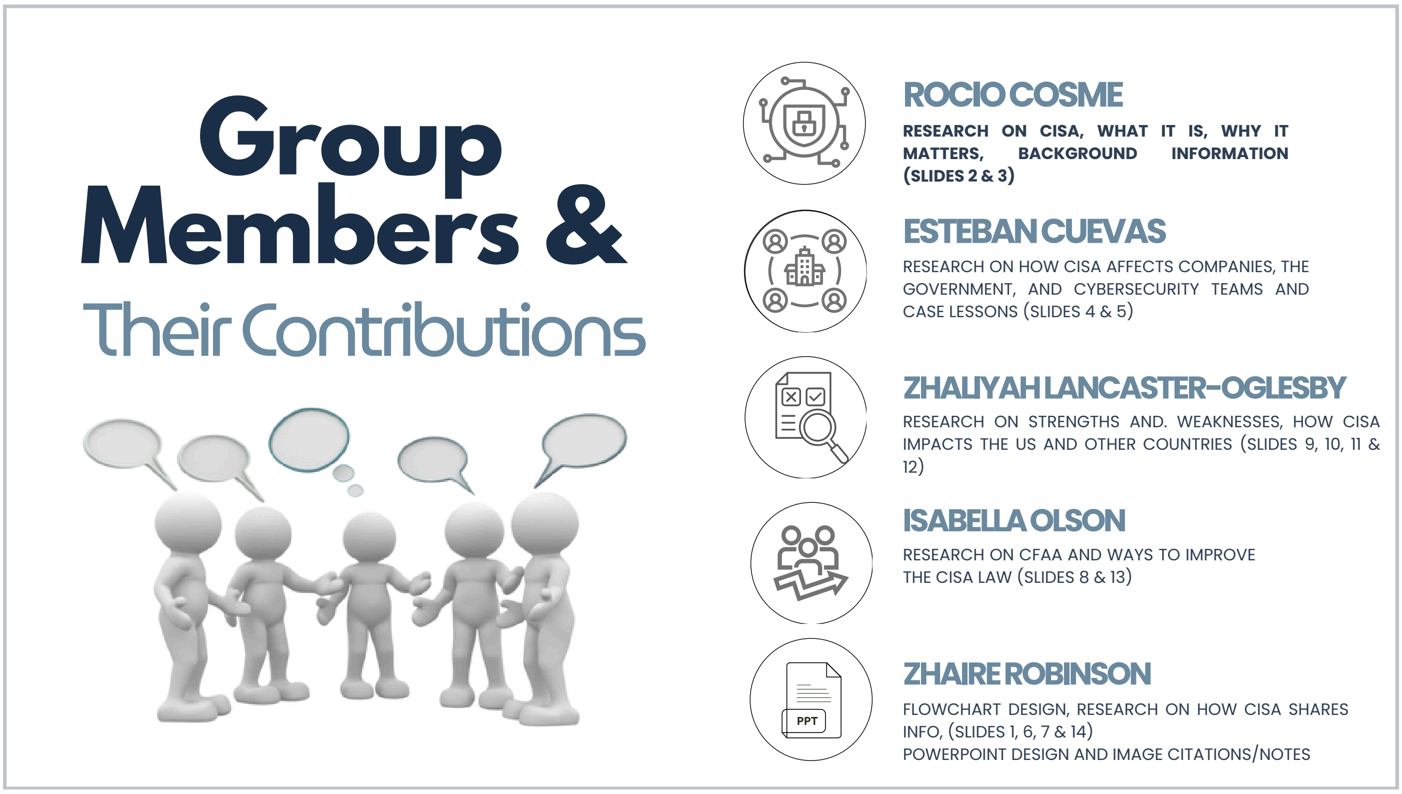
1.7.2013

CISA plays a crucial role in protecting national infrastructure, but I noticed that there are a few things it could adopt to work more efficiently.

First, CISA could improve by enhancing public–private collaboration. CISA needs to make information-sharing easier and faster so companies can respond to threats in real time.

Increasing funding and workforce development is essential. CISA could also modernize its threat intelligence systems by investing in AI and real-time analytics, they could detect and respond to threats faster. Automation can also help manage the massive amount of threat data they process daily.

‹#›



Group Members & Their Contributions

ROCIO COSME

RESEARCH ON CISA, WHAT IT IS, WHY IT MATTERS, BACKGROUND INFORMATION (SLIDES 2 & 3)

ESTEBAN CUEVAS

RESEARCH ON HOW CISA AFFECTS COMPANIES, THE GOVERNMENT, AND CYBERSECURITY TEAMS AND CASE LESSONS (SLIDES 4 & 5)

ZHALIYAH LANCASTER-OGLESBY

RESEARCH ON STRENGTHS AND. WEAKNESSES, HOW CISA IMPACTS THE US AND OTHER COUNTRIES (SLIDES 9, 10, 11 & 12)

ISABELLA OLSON

RESEARCH ON CFAA AND WAYS TO IMPROVE THE CISA LAW (SLIDES 8 & 13)

ZHAIRE ROBINSON

FLOWCHART DESIGN, RESEARCH ON HOW CISA SHARES INFO, (SLIDES 1, 6, 7 & 14)
POWERPOINT DESIGN AND IMAGE CITATIONS/NOTES

1.7.2013

As a team we sectioned off the research evenly, so that each person could have at least 2 slides to present their research and ideas.

This slide covers what each member worked on in this PowerPoint, and you can find their names at the bottom of each slide they researched.

‹#›