Cyber Innovation Ideation Initiative

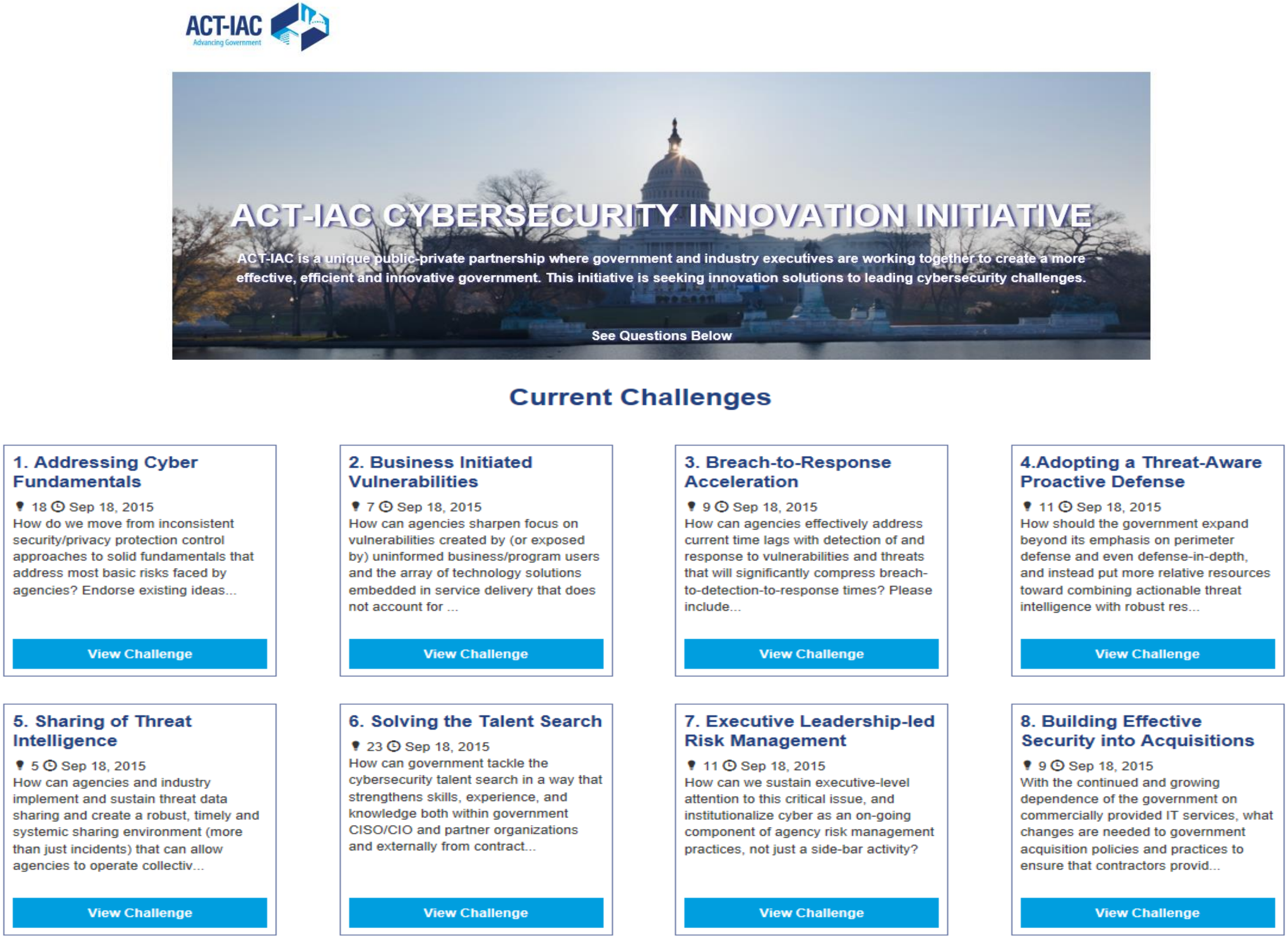
Agenda

- **Background on the Initiative**
- **Cross-cutting Themes**
- **Promising Ideas**
- **Next Steps**

Background

- Project to help improve Federal government's cybersecurity through innovative approaches
- Publicly accessible ideation platform used to collect recommendations from industry, government, academia and professional associations
- Ideas covered wide range of technical, policy, legal, operational, and managerial topics
- Focused on underutilized & new ways to improve Federal government cybersecurity
- Did not include information about specific products or services.
- Report provided to Federal CIO and posted on ACT-IAC's website at:
  - https://www.actiac.org/cyberinitiative

Ideation Platform



ACT-IAC CYBERSECURITY INNOVATION INITIATIVE

ACT-IAC is a unique public-private partnership where government and industry executives are working together to create a more effective, efficient and innovative government. This initiative is seeking innovation solutions to leading cybersecurity challenges.

See Questions Below

Current Challenges

1. Addressing Cyber Fundamentals

💡 18 🕒 Sep 18, 2015

How do we move from inconsistent security/privacy protection control approaches to solid fundamentals that address most basic risks faced by agencies? Endorse existing ideas...

View Challenge

2. Business Initiated Vulnerabilities

💡 7 🕒 Sep 18, 2015

How can agencies sharpen focus on vulnerabilities created by (or exposed by) uninformed business/program users and the array of technology solutions embedded in service delivery that does not account for ...

View Challenge

3. Breach-to-Response Acceleration

💡 9 🕒 Sep 18, 2015

How can agencies effectively address current time lags with detection of and response to vulnerabilities and threats that will significantly compress breach-to-detection-to-response times? Please include...

View Challenge

4.Adopting a Threat-Aware Proactive Defense

💡 11 🕒 Sep 18, 2015

How should the government expand beyond its emphasis on perimeter defense and even defense-in-depth, and instead put more relative resources toward combining actionable threat intelligence with robust res...

View Challenge

5. Sharing of Threat Intelligence

💡 5 🕒 Sep 18, 2015

How can agencies and industry implement and sustain threat data sharing and create a robust, timely and systemic sharing environment (more than just incidents) that can allow agencies to operate collectiv...

View Challenge

6. Solving the Talent Search

💡 23 🕒 Sep 18, 2015

How can government tackle the cybersecurity talent search in a way that strengthens skills, experience, and knowledge both within government CISO/CIO and partner organizations and externally from contract...

View Challenge

7. Executive Leadership-led Risk Management

💡 11 🕒 Sep 18, 2015

How can we sustain executive-level attention to this critical issue, and institutionalize cyber as an on-going component of agency risk management practices, not just a side-bar activity?

View Challenge

8. Building Effective Security into Acquisitions

💡 9 🕒 Sep 18, 2015

With the continued and growing dependence of the government on commercially provided IT services, what changes are needed to government acquisition policies and practices to ensure that contractors provid...

View Challenge

Content/Ideas Submitted

- 127 submissions, many containing multiple ideas
- Sources included industry, government, academia, and professional associations
- Additional ideas collected at ACT-IAC membership meetings
- Ideas reviewed and compiled by five teams comprised of 45 ACT-IAC members
- Team members also added their own ideas

Cross-cutting Themes

- Much of what is required is known but not implemented; reinforce basics
- Cyber professionals and mission program executives need to work together more closely
- Chief Risk Officers, Chief Data Officers, CIOs, and CISOs need to work together closely
- Current cyber training is insufficient; increase emphasis on developing competencies, practicing tactics and procedures, and sharing cyber knowledge
- Enhanced, timely sharing of threats, incidents, and solutions/responses between industry and government is essential

Promising Ideas

Question 1
Addressing Cyber Fundamentals

How do we move from inconsistent security/privacy protection control approaches to solid fundamentals that address most basic risks faced by agencies?

1. **Embrace Cyber "Tips of the Day"** -- Used on intranet home web page, in staff mtgs, blogs, etc. These would be focused on knowledge leveling, increasing awareness of vulnerabilities created by SPAM/Phish attacks, etc.

2. **Adopt Cyber Investment Management Boards** (DOD example) where cyber projects are presented, defended, and measured against outcome based performance measures for funding. Helps get cybersecurity accountability as a shared responsibility across senior leadership of the organization and to understand costs and risk benefits. Use new board or existing one.

3. **Recommend SEC-type self-assessment checklist** to ensure sound execution. Leverage the self audit capability of the SEC as a guidance for other agencies. https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf

Promising Ideas

Question 2

Business Initiated Vulnerabilities

How can agencies sharpen their focus on vulnerabilities created by (or exposed by) uninformed business/program users and the array of technology solutions embedded in service delivery that does not account for cyber?

1. **Build a Security Maven approach similar to Wal Mart.** Walmart's security mavens were not security experts, but members of development teams trained and deputized to be first level support on security for development teams. The mavens dramatically scaled security's ability to support the teams.

2. **Build security into the front end of development activities** so that tailored standards could be used to address appropriate risk factors in test/dev settings – create DMZ for developers, who build knowing security policies in advance.

3. **Adopt a risk-based approach using quantifiable risk measures in Tech-Stat and similar session**s. Using CISO/biz lead collaboration, mission/business requests involving business process changes or introduction of new products/apps would be properly vetted for security risks.

Promising Ideas

Question 3
Breach-to-Response Acceleration

How can agencies effectively address current time lags with detection of and response to vulnerabilities and threats that will significantly compress breach-to-detection-to-response times? Please include ideas on how government agencies can expand capabilities beyond reacting to known threats through programs like Einstein, to identify new threats and zero-day exploits in near real-time.

1. **Data anomalies** – Agencies monitor data flows, especially outgoing data, for anomalies (include tagging for PII and sensitive data). This would have been a signal to spot exfiltration like in the OPM case.

2. **Create a "hotline" reporting channel** for people who suspect an issue, in agency or government-wide – if a user sees a potential problem, can check with team to for tech assistance on whether it's real and what are next steps. Akin to a help desk for cyber reporting.

3. **Broaden Incident/Response awareness, training, action planning**. Employees should practice cyber response regularly as part of emergency preparedness, and provide feedback on plans, training, and exercises. Exercise evaluation activities should be managed independently of the response organization, to avoid a potential conflict of interest if the reviewing entity resides within the operational entity.

Promising Ideas

Question 4
Adopting a Threat Aware Proactive Defense

How should the government expand beyond its emphasis on perimeter defense and even defense-in-depth, and instead put more relative resources toward combining actionable threat intelligence with robust response and resiliency strategies and architectures that account for the adversary's point of view?

1. **Create Blue Team audits followed by Red Team operations,** performed by pre-qualified contractors or in-house staff using efficient contract services vehicle managed by GSA. Focus is beyond standard penetration testing and embraces "hunting" tactics largely used by DOD Red Teams to emulate adversaries. Increases resiliency and ability to enhance capability to address early indicators of APTs.

2. **Distributed Corroboration of Service (DCOS)** – use big data and machine learning to quickly share info on DDOS attacks for rapid adaptation and response. The "machine learning" would use a service such as *http://map.norsecorp.com* to see where attacks are coming from the types and successes, and alert the community of the attack vectors and assess the current networks ability to sustain the attack.

3. **Pursue insider threat strategy –** Develop an insider threat action plan, including such measures as: (1) Detect malicious cyber insiders that aren't detectable by other means; (2) find cases of compromised credentials by spotting suspicious changes in employee behavior, (3) track risky behavior that puts the organization at risk, and (4) use security tools to deliver other benefits to the business, such as dramatic savings in IT budgets.

Promising Ideas

Question 5
Sharing of Threat Intelligence

How can agencies and industry implement and sustain threat data sharing and create a robust, timely and systemic sharing environment (more than just incidents) that can allow agencies to operate collectively government-wide and with industry and in real time rather than independently with little peripheral view of threats and responses?

1. **Endorse and expand STIX / TAXII** so that data breach reporting is more robust and shared widely but in meaningful ways.
   -- Embrace operations similar to that used by North American Network Operators Group that shares incidents across most of the major networks in the US
   -- Include a "neighborhood cyber watch" program where companies and citizens can report issues to a shared resource that then shares with appropriate authorities.

2. **Establish an environment that facilitates threat data information sharing**; it still operates in silos. Action must be taken to arm stakeholders with needed information to make decisions and take necessary actions to maintain enterprise situational awareness (know the attacker, their methodology, and their targets), protect and defend their networks, respond and recover to threats and incidents, and manage/mitigate cybersecurity-related risks.

STIX is Structured Threat Information Expression
TAXII is Trusted Automated Exchange of Indicator Information
See https://www.us-cert.gov/Information-Sharing-Specifications-Cybersecurity

Promising Ideas

Question 6
Solving the Talent Search

How can government tackle the cybersecurity talent search in a way that strengthens skills, experience, and knowledge both within government CISO/CIO and partner organizations and externally from contracted services?

1. **Create a Cyber Corps** -- Create an elite CyberSec Reserve Corps that have passed necessary screening that can be used by government on challenging security projects. Use as a recruiting tool for new graduates; aggressively recruit them to be part of this group or high visibility internships with return of visibility, rich career enhancing assignments, college loan repayment, etc.

2. **Look for talent in other parts of the organization** that could be used by cybersec shops w/o having to hire: risk management skills, analytical skills, cost/benefit analyses. Retool as needed for cyber roles.

3. **Provide an environment of skills-based and performance-based training where cyber supports the mission, through** functional assessments and exercise events can occur that benefit cyber talent levels for all employees. Expand from knowledge-based technical training in certifying federal employees and contractors in their job duties.

Promising Ideas

Question 7

Executive Leadership-led Risk Management

How can we sustain executive-level attention to this critical issue, and institutionalize cyber as an on-going component of agency risk management practices, not just a side-bar activity?

1. **Adapt private sector Board of Directors oversight model.** Utilize a Board Room check-list for determining adequacy of security-to-risk decisions. Agency leadership would be accountable and would assess every quarter.

2. **Cyber RACI** -- Provide for the escalation of risk-based decisions through senior leadership if critical security recommendations are rejected by owners of business lines or applications, ensuring critical security decisions are not made in isolation. Establish a RACI-type (responsible, accountable, consulted, informed) chart for the overall federal government and each department and agency that clearly identifies roles, responsibilities, and accountabilities for cybersecurity.

3. **Use FITARA governance** requirements to get cyber risks built into program and budgeting evaluations up front, not afterwards

Promising Ideas

Question 8
Build Effective Security into Acquisitions

With the continued and growing dependence of the government on commercially provided IT services, what changes are needed to government acquisition policies and practices to ensure that contractors provide adequate security and privacy protections to government data and information?

1. **Determine the viability of requiring federal contractors to have cyber insurance** or, alternatively, make it a + evaluation factor in bid assessments.

2. **Get R&D activities in cyber being done in government and quasi-government labs (DARPA, DHS S&T, NIST, etc.) placed into acquisition availability faster**. Issue challenges to the government and commercial labs to address specific cyber capability needs

3. **Use certifications similar to FedRAMP** (standard baseline assessment) for all IT acquisitions, not just for cloud.

4. **Develop and propagate model cyber contract requirements language** which among other things, addresses secure supply-chain issues.

Next Steps

- ACT-IAC Communities of Interest developing action plans to address report ideas about:
  - Cyber Workforce
  - Integrating Cyber into Acquisitions
- In near future, after new OMB Guidance, address:
  - Risk Management
  - Incident Response
- Upcoming ACT-IAC conferences and forums will include deeper treatment of ideas from the report

Strengthening Federal Cybersecurity: Results of the Cyber Innovation Ideation Initiative

December 2015