ETAAC Public Meeting
March 24, 2011

ETAAC Software Subcommittee

Summary of Recommendations relating to the Security of the e-File Digital Infrastructure

This document summarizes the key recommendations of the Software Subcommittee Security Working Group. The full description of our recommendations are contained in our final written report, which should be considered the authoritative description. As a result, this summary should not be quoted by third parties.

Today's review

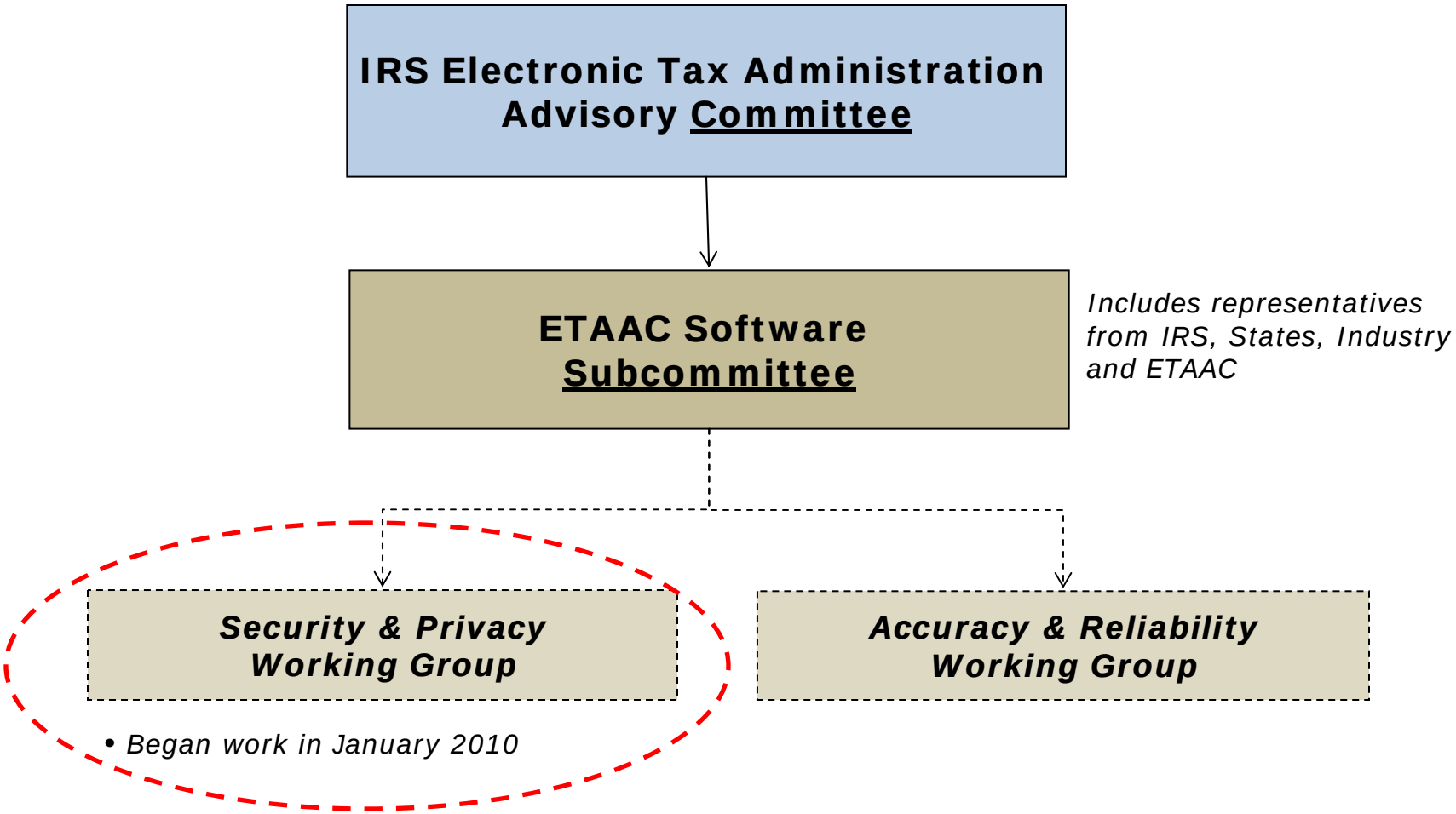
- **Objective:** Report the security recommendations of the ETAAC Software Subcommittee's Security Working Group

- **Today's summary report**
  - Brief Background Review – summarizing December 2010 report out
  - Unanimous recommendations relating to IRS' questions:
    - Standards
    - Review Process
    - Validation
    - Implementation

Note: Detailed recommendations included in Working Group's written report

Brief Background Review

ETAAC Security & Privacy Working Group

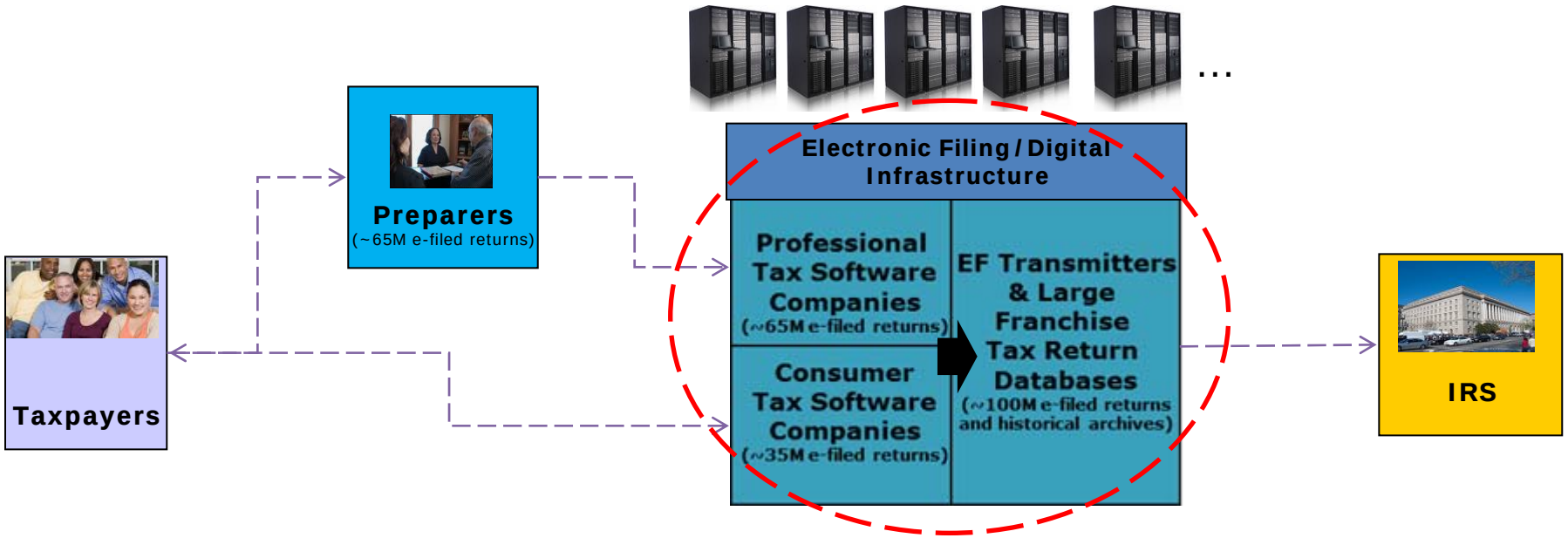


Security is important…
Security programs are already required

- 100% of federal e-filed individual returns are generated by private industry
- Security and privacy concerns affect taxpayer decisions to e-file
- All Authorized IRS e-file Providers are <u>currently</u> required by FTC Safeguards Rule to have *comprehensive information security program*
  - ✓ Designated staff
  - ✓ Risk assessments
  - ✓ Safeguards assessments
  - ✓ Testing & monitoring
  - ✓ Third party oversight
  - ✓ Ongoing program adjustment as environment changes
- **<u>How</u>…not <u>whether</u> companies should be subject to security requirements**

We set our initial focus on the e-file "digital infrastructure"

Considered highest risk area given high volume of electronic returns, <u>but</u> industry diversification helps to mitigate risks



<u>Hundreds</u> of "digital participants" processing ~100M+ returns

ETAAC can consider other areas in the future

IRS asked for our recommendations in four key areas

1. **Standards:** What additional guidance or standards should IRS set in connection with the current responsibility of Authorized IRS e-file Providers to comply with the FTC Safeguards Rule?

2. **Assessment:** What assessment methodology should IRS require to ensure that Providers are complying with the FTC Safeguards Rule and any other relevant security standards?

3. **Validation:** What approach should IRS take to ensure that it is informed whether a particular company has successfully completed any security review and is meeting applicable standards?

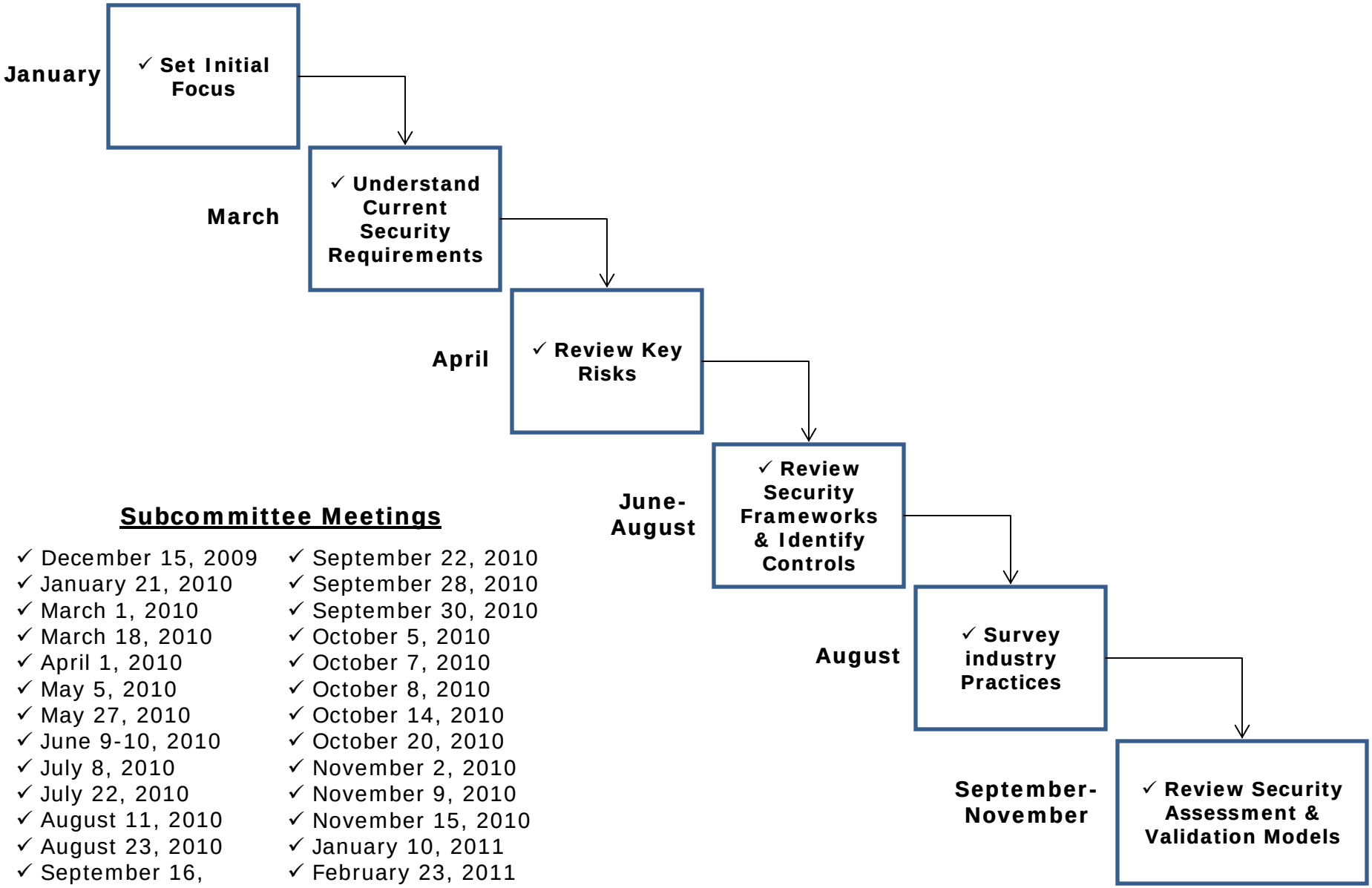
4. **Implementation:** What plan/schedule should IRS follow to implement any new security requirements in this area?

As reported at December 2010 ETAAC Public Meeting, we followed a rigorous, deliberative approach…

Information considered by the Working Group…

- IRS e-file Provider security requirements
- Reports on security threats, risks, and implications
- Security frameworks/ requirements (with outside experts)
- Qualitative feedback from industry on current security practices
- A broad array of industry and government security assessment models
- FTC Safeguards Rule enforcement actions (with FTC staff)

...including over 25 meetings and a commitment of well over 1,000 hours



Subcommittee Meetings

- ✓ December 15, 2009
- ✓ January 21, 2010
- ✓ March 1, 2010
- ✓ March 18, 2010
- ✓ April 1, 2010
- ✓ May 5, 2010
- ✓ May 27, 2010
- ✓ June 9-10, 2010
- ✓ July 8, 2010
- ✓ July 22, 2010
- ✓ August 11, 2010
- ✓ August 23, 2010
- ✓ September 16, 2010
- ✓ September 22, 2010
- ✓ September 28, 2010
- ✓ September 30, 2010
- ✓ October 5, 2010
- ✓ October 7, 2010
- ✓ October 8, 2010
- ✓ October 14, 2010
- ✓ October 20, 2010
- ✓ November 2, 2010
- ✓ November 9, 2010
- ✓ November 15, 2010
- ✓ January 10, 2011
- ✓ February 23, 2011

…and arrived at some key conclusions

- Attractive Data Target
- Breaches Affect Confidence
- Safeguards Rule Provides High Level Framework
- IRS should Supplement Self Interest
- Controls + Assessments = Reasonable Assurance
- Balance Benefit / Burden
- Seasonality and Deadline Factors
- Start with Education & Collaboration

Substantive & Implementation Recommendations

Summary of Substantive Recommendations

1. Scope. These recommendations focus on:
   - E-file "digital infrastructure" participants, and
   - The tax information they store or process.
2. Standards. IRS should supplement the FTC Safeguards Rule with specific NIST SP 800-53 security controls.
3. Assessment. IRS should require periodic self and third party security assessments.
4. IRS Validation. IRS must actively monitor the ongoing conduct and effectiveness of the program.

Recommendation details follow…

Substantive Recommendation #1
Scope

- **Who** - IRS E-File Program Digital Infrastructure Participants
  - Transmitters
  - Software Developers
  - Online Providers
  - Intermediate Service Providers
- **What** - Taxpayer accounts and personal information
  - Initial phase relates to individual and business income tax returns.
  - Employment returns (94X series) or information returns deferred for later consideration
- **Where** - Taxpayer Data Environment
  - Any network component, server, application or IT asset (e.g., laptops, servers, workstations, databases) included in or connected to the taxpayer data environment.
  - By association, related organizational, physical environment and process components become part of the security program scope.

Substantive Recommendation #2
Standards

- Require the implementation of selected NIST SP 800-53 controls
  - Balance of flexibility and specificity that industry needs
  - "Appropriate" is defined based on who is in scope
- Selected NIST 800-53 controls are chosen based on their contributions to enhancing information security and their relevance to industry
- Defer consideration of those NIST "CP" and "PE" controls relating to systems reliability such as disaster recovery
  - ETAAC can consider these areas as it assumes the work of the Subcommittee

Substantive Recommendation #3
Assessment

- **Accountability**
  - Company senior management is accountable for implementing a comprehensive information security program
- **Certification / Reasonable Assurance**
  - Senior management should annually certify that the company has *reasonable assurance* of the security, confidentiality, and integrity of personal information
- **Assessment Cycle**
  - Annual *self-assessment* conducted by a qualified person, and
  - A triennial *independent third party assessment* by a qualified person.
  - IRS could require that a third party assessment be conducted more frequently based on risk or other factors established by IRS.
- **Reporting**
  - Companies should be required to report the results of their annual self-assessments and any periodic third party assessments to IRS.

Substantive Recommendation #3
Assessor Qualifications

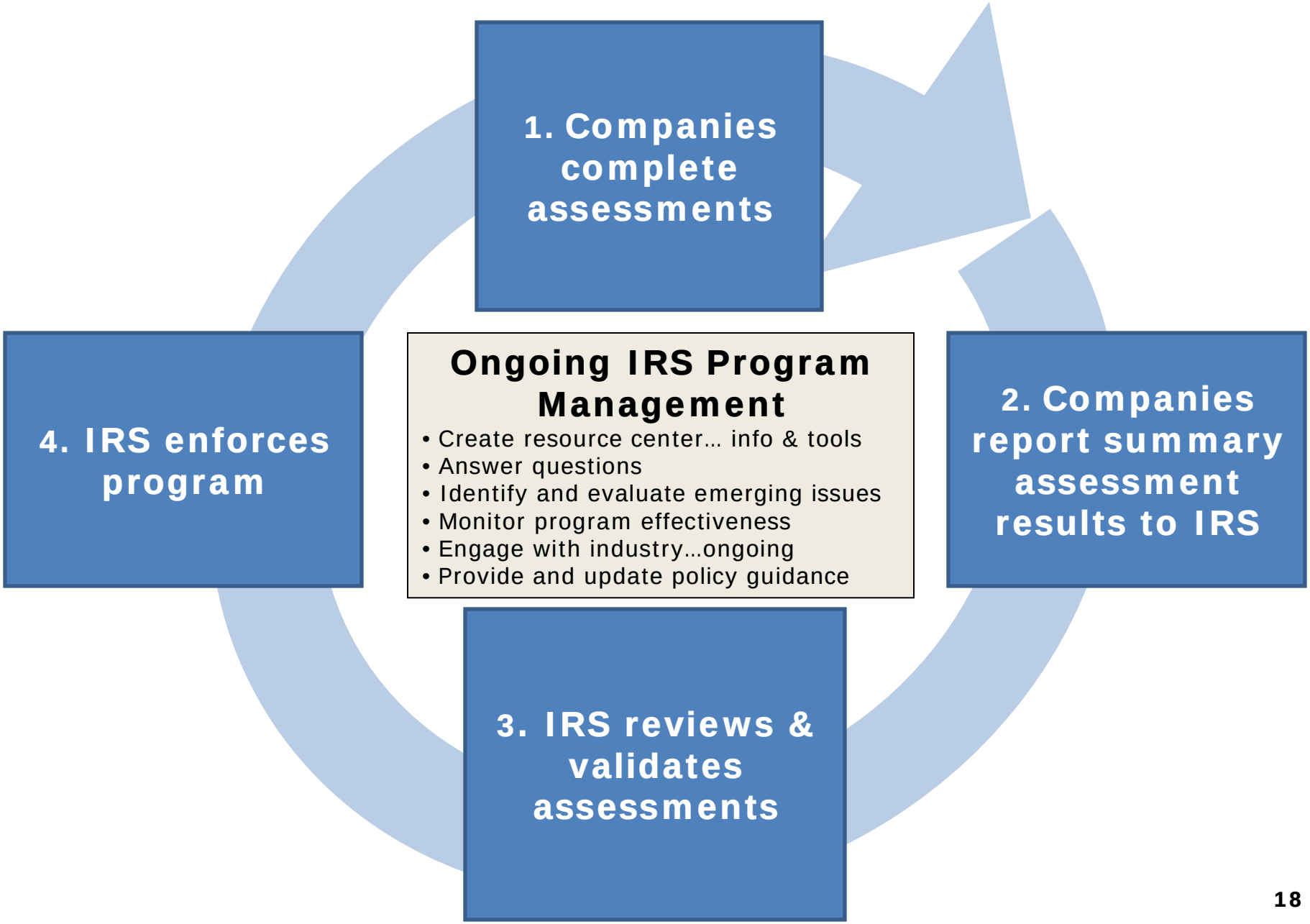
- **Self-assessor qualifications**
  - *College Degree*
  - *Company IT Systems Experience* – minimum 3 years
  - *Security IT Experience* – minimum 3 years

- **Third party assessor qualifications**
  - *Active Business Requirement*
  - *Professional & Ethical Standards*
  - *Certification & Experience Requirements*
    - Security certifications such as: CISSP, CISA, CISM, GSEC, GISP or QSA, and
    - At least 5 years experience

Substantive Recommendation #4
IRS Validation

- IRS should conduct "spot checks" of company and assessor performance and practices based on a variety of factors
  - Risk-based -- probability vs. impact
    - Check companies that have a *higher probability* of a security breach
    - Security breaches that would have *high impact*
  - Random selection
    - IRS should "spot check" both self-assessments and third party assessments on a random basis, e.g., a specified percentage of assessments every year
  - Event-driven
    - Companies whose security programs are in question based on complaints (users/customers, competitors, etc.), events (breach notifications), etc.
- Adverse spot checks should have consequences
  - Increased frequency for third party assessments
  - Suspension of company from the e-file program or other IRS enforcement actions
  - Prohibition on assessors being used for third party assessments

IRS's critical role in a *living process*



Summary of Implementation Recommendations

1. **Guiding Principles:** IRS should develop and implement any guidance and standards consistent with the guiding principles articulated in ETAAC's 2009 Annual Report to Congress.
2. **Regulatory Implementation Process:** IRS must determine the appropriate regulatory mechanisms to implement any new guidance or standards, and create an effective outreach program to accelerate company compliance.
3. **Implementation Phase-in:** IRS should phase-in the effectiveness of its guidance and new requirements over a two to three year period.

Recommendation details follow…

Implementation Recommendation #1
Guiding Principles

IRS guidance and standards should be consistent with certain guiding principles, including those articulated in ETAAC's 2009 Annual Report to Congress:

- Use existing, recognized security standards
- "Controls based," not technology prescriptive
- Clear requirements
- Minimizing duplication with existing company security assessments
- Early directional signals from IRS
- Progressive implementation stages
  - Early outreach and collaboration
  - Education and validation of results
  - Reserve sanctions for egregious cases

Implementation Recommendation #2
Regulatory Implementation Process

- Joint public/private effort to streamline compliance processes and procedures to reduce cost and increase effectiveness
- IRS must determine the appropriate regulatory mechanism to implement any new requirements…
  - New or expanded regulations
  - IRS Revenue Procedure, etc.
- Support mechanism with outreach and collaboration
  - Help companies move quickly towards effective program
  - Identify and promulgate helpful guidance on implementing new requirements
  - Create a forum and process for raising questions and issues, resolving conflicting points of view, and making decisions publicly accessible

Implementation Recommendation #3
Implementation Phase-in

Companies <u>immediately</u> begin providing self-assessment certifications

PROGRAM LAUNCH
- ✓ Program Development
- ✓ Initial outreach
- ✓ Program launch
- ✓ FTC Safeguards <u>self-certification</u>

1

END OF "YEAR 1"
- ✓ Ongoing outreach
- ✓ NIST Priority 1 Controls implementation completed
- ✓ FTC Safeguards <u>self-certification</u> inc'l NIST Priority 1 Controls

2

END OF "YEAR 2"
- ✓ Ongoing outreach
- ✓ NIST Priority 2 Controls implementation completed
- ✓ FTC Safeguards <u>self-certification</u> inc'l NIST Priority 1 & 2 Controls

FULL IMPLEMENTATION

3

END OF "YEAR 3"
- ✓ Ongoing outreach
- ✓ NIST Priority 3 Controls implementation completed
- ✓ FTC Safeguards <u>third party</u> certification inc'l NIST Priority 1, 2 & 3 controls

Summary of Recommendations

	SELF-ASSESSMENT	THIRD PARTY ASSESSMENT
Security Controls being Assessed	Specified NIST 800-53 controls	
Testing Procedures	Specified testing procedures based on IRS Safeguards and NIST 800-53A	
Qualified Assessor	*Certification and experience requirements as designated by IRS.*	*Certification, experience and independence requirements as designated by IRS.*
Frequency of Assessment	*Annually*	*Every 3 years*
Level of Certification	*Reasonable Assurance* based on the implementation of the recommended standards, procedures and assessments	
Certifying Party	*(i) Qualified Self-assessor, and (ii) either CEO or, in a large company, the senior officer responsible for the business*	*(i) Qualified independent third party assessor, and (ii) either CEO or, in a large company, the senior officer responsible for the business*
Reported to IRS	Yes	

Questions & Discussion

Appendix

Subcommittee-recommended NIST controls

- Access Control: AC1, AC2, AC3, AC4, AC5, AC6, AC7, AC8, AC11, AC17, AC18, AC19
- Awareness and Training: AT1, AT2, AT3, AT4, AT5
- Audit and Accountability: AU1, AU2, AU3, AU5, AU6, AU7, AU8, AU9, AU11
- Certification, Accreditation and Security Assessments: CA1, CA2, CA3, CA5, CA6, CA7
- Configuration Management: CM1, CM2, CM3, CM4, CM5, CM6, CM7, CM8
- Identification and Authentication: IA1, IA2, IA3, IA4, IA5, IA6, IA7
- Incident Response : IR1, IR2, IR3, IR4, IR5, IR6, IR7
- Maintenance : MA1, MA2, MA4, MA5
- Media Protection: MP1, MP2, MP3, MP4, MP5, MP6
- Physical and Environmental Protection : PE1, PE2, PE3, PE4, PE5, PE6, PE7, PE8, PE13, PE16
- Program Management: PM1, PM2, PM9
- Personnel Security: PS1, PS2, PS3, PS4, PS5, PS6, PS7, PS8
- Risk Assessment: RA1, RA2, RA3, RA5
- System and Services Acquisition : SA3, SA5, SA7, SA8, SA9, SA10, SA11
- System and Communications Protection: SC1, SC2, SC4, SC7, SC8, SC9, SC10, SC12, SC13, SC17, SC18, SC19, SC23, SC24, SC28
- System and Information Integrity: SI1, SI2, SI3, SI4, SI5, SI8, SI11

Note: The Subcommittee has deferred the consideration of any NIST “CP” and “PE” controls relating to systems reliability (availability, disaster recovery, etc.) to the Subcommittee’s Accuracy/Reliability Working Group.

Implementation Phase-in

We recommend phasing in the selected NIST 800-53 controls over a 2-3 year period in the following prioritized order:

- **Priority 1 Controls (first 12 months):** AC, AT, IA, IR, PE, PS, SC & SI
  - AC: Access Control
  - AT: Awareness and Training
  - IA: Identification and Authentication
  - IR: Incident Response
  - PE: Physical and Environmental Protection
  - PS: Personnel Security
  - SC: System and Communications Protection
  - SI: System and Information Integrity
- **Priority 2 Controls (following 12 months):** AU, CA, CM, MP, PM, RA
  - AU: Audit and Accountability
  - CA: Certification, Accreditation, and Security Assessments
  - CM: Configuration Management
  - MP: Media Protection
  - PM: Program Management
  - RA: Risk Assessment
- **Priority 3 Controls (following 6 months):** MA, SA
  - MA: Maintenance
  - SA: System and Services Acquisition