Integrating Privacy into the Risk Management Framework

Celeste Dade-Vinson, Privacy Officer, National Institutes of Health

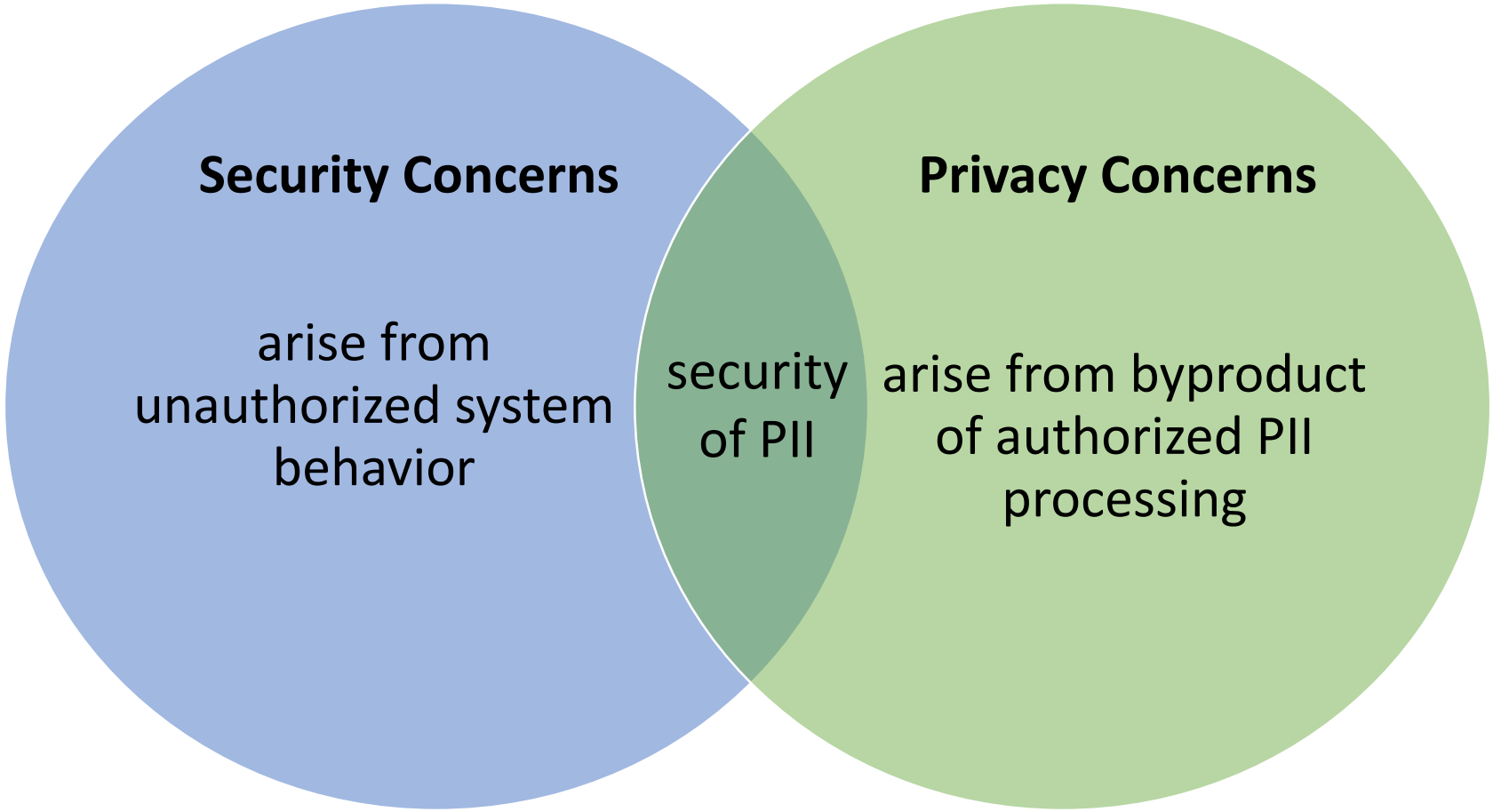
Jamie Danker, Director of Privacy, Easy Dynamics Corporation

Elizabeth Koran, Privacy Policy Analyst, Department of Health and Human Services

Disclaimers

The views and opinions expressed in this discussion are those of the individual presenters and should not be attributed to their employers.

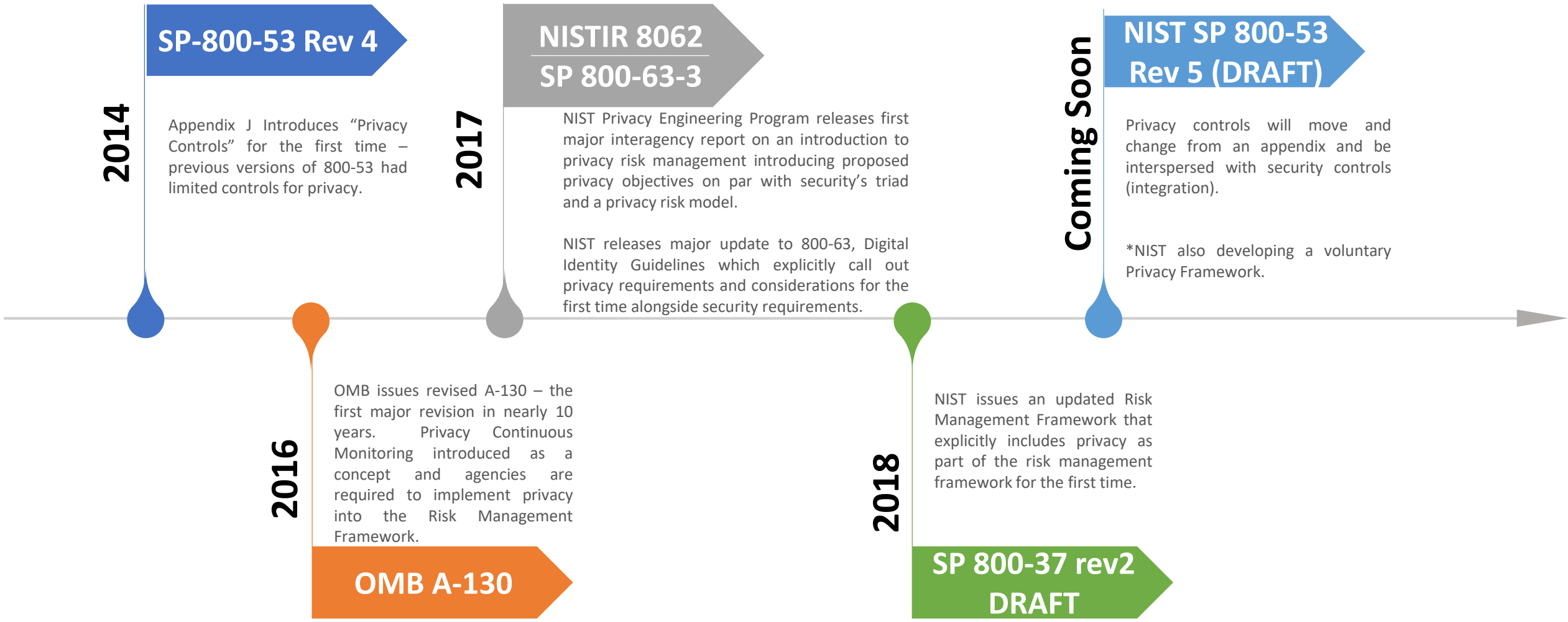
Information Security and Privacy: Boundaries and Overlap



OMB Circular A-130

“While security and privacy are independent and separate disciplines, they are closely related, and it is essential for agencies to take a coordinated approach to identifying and managing security and privacy risks and complying with applicable requirements….”

Privacy Integration into Risk Management

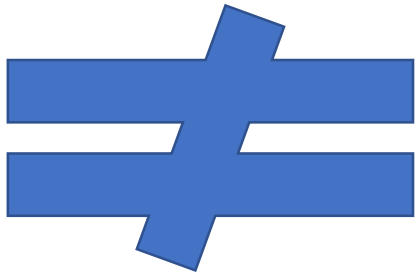


Common Challenges to Implementing Privacy Into the Risk Management Framework

- Security and privacy conflation
- Privacy program structure and resources
- Stakeholder communication
- Privacy control assessments
- Privacy continuous monitoring

Overcoming Challenges: Security and Privacy Conflation

Confidentiality



Privacy

Overcoming Challenges: Structure, Resources, and Communication

Source: Still of Kristen Wiig in Bridesmaids. https://www.buzzfeed.com/mariahoxley/signs-youre-not-actually-broke-youre-just-rich-poor

- Privacy responsibilities are often distributed across multiple organizations.
- Privacy programs tend to have limited resources.

Lessons Learned

- Communicate across boundaries.
- Work together with privacy and security teams and even other agencies to leverage existing resources or to combine efforts to create new ones.
- Integrate privacy and security policies to create buy-in.
- Build relationships now to prepare your organization for NIST SP 800-53 Rev 5.

Overcoming Challenges: Privacy Control Assessment Criteria

- NIST has not issued assessment guidance for the privacy controls.
- Concurrent SAOP and AO approval requires new procedures.
- Assessors are unlikely to be privacy SMEs.
- Many controls aren't technical.

Lessons Learned

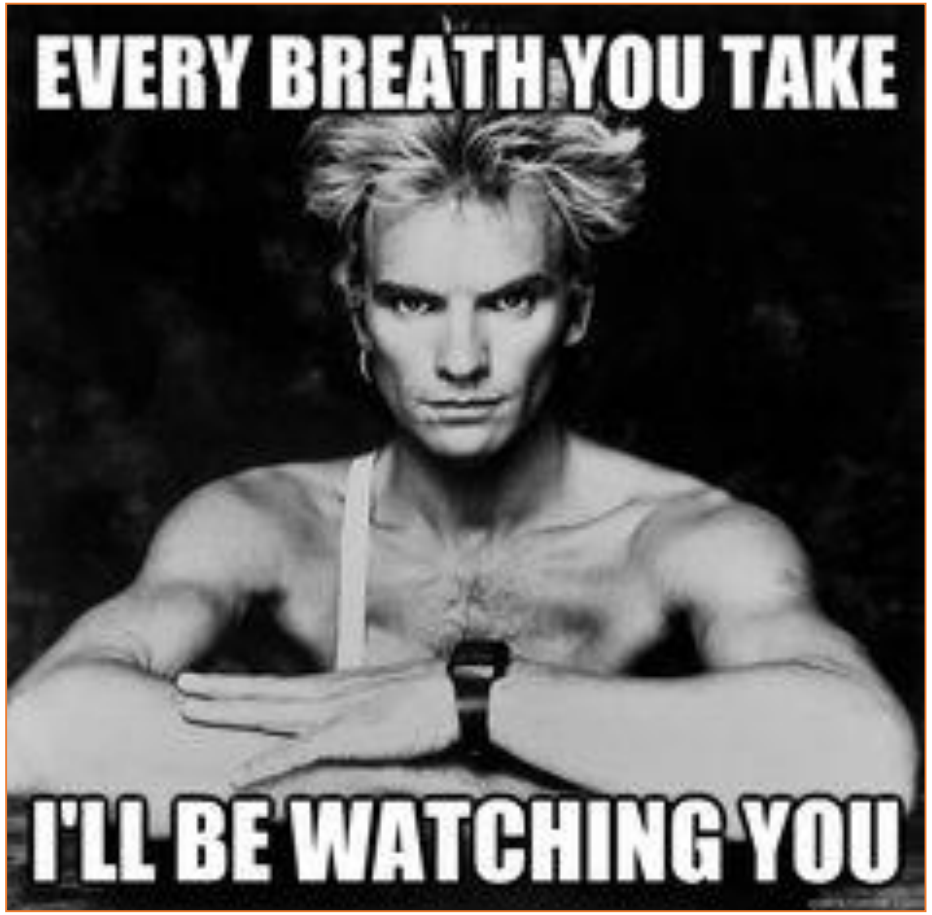
- Crosswalk the privacy controls and any existing privacy compliance documentation.
- Develop resources that help both assessors and privacy officers.

Overcoming Challenges: Privacy Continuous Monitoring

- Privacy is required to assess at a frequency sufficient to ensure compliance and manage risk.
- Most controls do not lend themselves to automated monitoring.
- Frequency may also be driven by factors like regular audits or reports.

Lessons Learned

- Align your PCM with your organization's ISCM. Work with security to identify what you can automate.
- If your controls and PIAs are aligned, you have a built in minimum cadence.



Source: Photograph of Sting. https://goo.gl/images/p2K1TK

Takeaways

- Privacy and security need to learn from each other and become allies.
- Integrate and leverage as much as possible – this will help save resources and prepare your organization for NIST SP 800-53 Rev 5.
- Understand that it’s a work in progress.

Questions?

Contacts

- Celeste Dade-Vinson: celeste.dade-vinson@nih.gov
- Jamie Danker: jdanker@easydynamics.com
- Elizabeth Koran: elizabeth.koran@hhs.gov