

Retiring use of Weak Encryption

As of May 18, 2021

Zeenath Fernandes

Sr. Lead, Enterprise Information Security

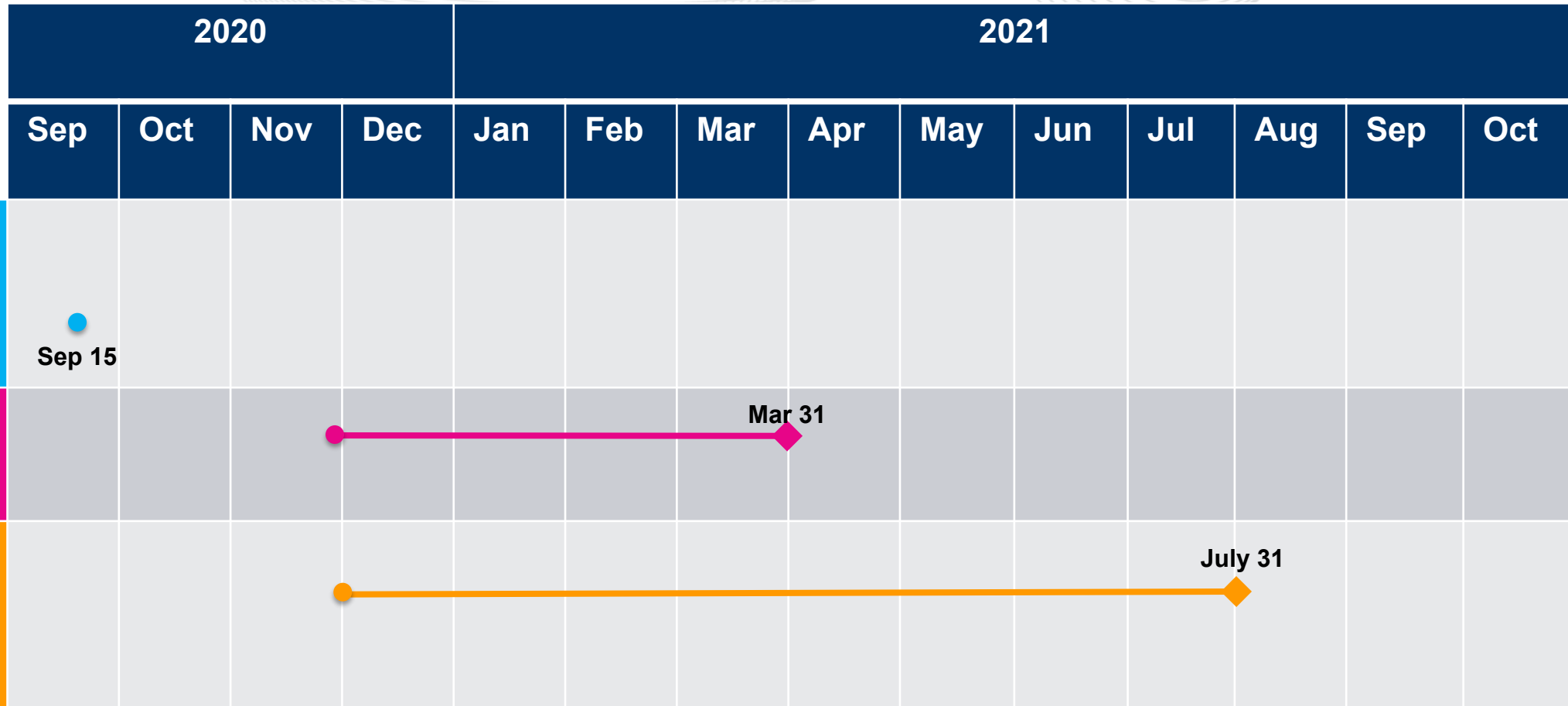
- Train Browser and Browserless Rollout Successfully Completed on April 29
- Weak Encryption Remediation Guide Available at <https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx>

Product - Action Required	Deadline	Who May Be Affected
<p>PJM requests that each company update the encryption on the source devices to use an acceptable level of encryption documented in https://www.pjm.com/-/media/etools/security/weak-encryption-remediation-guide.ashx.</p>	<p>Production November 1 browser and browserless systems</p>	<ul style="list-style-type: none"> • Participants who use PJM’s internet facing tools and use weak encryption cipher suites on their source devices. • 94% of encrypted sessions are already strong and are not affected.





Roadmap for Elimination of Weak Encryption

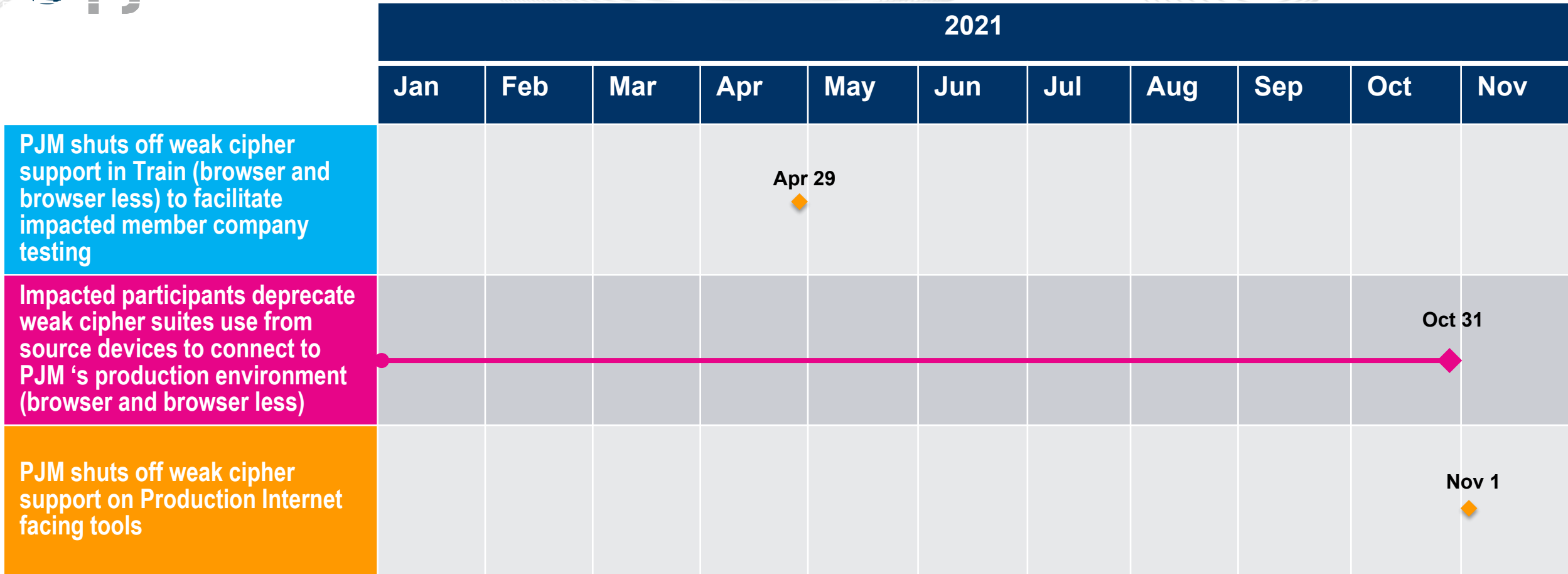


Legend

- Start Date
- ◆ End Date



Roadmap for Elimination of Weak Encryption



Legend

- Start Date
- ◆ End Date

- National Security Agency (NSA) Recommendation:
 - [Eliminating Obsolete Transport Layer Security \(TLS\)](#)
- 3DES was deprecated by the National Institute of Standards and Technology in 2017. An established reference can be found here:
 - <https://csrc.nist.gov/news/2017/update-to-current-use-and-deprecation-of-tdea>
- TLS 1.0 and TLS 1.1 were released in 1999 and 2006 respectively. Security flaws in design of TLS 1.1 lead to the release of TLS 1.2 in 2008.
 - In October 2018, Apple, Google, Microsoft, and Mozilla jointly announced they would deprecate TLS 1.0 and 1.1 in March 2020.
 - An overview of TLS can be found here:
 - https://en.wikipedia.org/wiki/Transport_Layer_Security
- TLS_RSA_* – Site describing method to attack this cipher suite can be found at <https://robotattack.org/>.

- PJM will no longer support the TLS 1.0 or TLS 1.1 protocols.
- PJM will no longer support the 3DES cipher and the TLS_RSA_* ciphers in TLS 1.2.
 - Members need to upgrade the encryption used on systems that connect to PJM externally facing systems.
 - Browser and browser less support will stop on April 29 2021 in Train
 - Browser and browser less support will stop on Nov 1 2021 in Production
- These encryption mechanisms are no longer secure.

- PJM has supplied Weak Encryption Remediation Guide to member companies.
- PJM has shut off weak cipher support in Train (browser and browser less) to facilitate member company testing.
- Impacted member company should contact PJM's [member relations](#) to verify list of sources and discuss next steps. The target date of completion is July 31 2021.
- Questions or feedback can be sent to: TechChangeForum@pjm.com.

Presenter:

Zeenath Fernandes

Zeenath.Fernandes@pjm.com

SME:

Zeenath Fernandes

Zeenath.Fernandes@pjm.com

Retiring use of Weak Encryption



Member Hotline

(610) 666 – 8980

(866) 400 – 8980

custsvc@pjm.com