IDENTIV + THURSBY Software

Solutions Brief

SECURE MOBILE AUTHENTICATION

NIST 800-172 COMPLIANCE

Identiv's NIST 800-172 compliance solution for wireless users accessing CUI focuses on secure mobile authentication and encryption.

The National Institute of Standards and Technology (NIST) Special Publication 800-172 calls out the security requirements all organizations must adhere to when accessing controlled unclassified information (CUI) — sections 3.1.16 through 3.1.22 define the specific requirements for wireless users and access.

Wireless users of CUI must protect the information being accessed using authentication and encryption. That means, per NIST 800-172, if you're accessing CUI, you must control the connection of mobile devices, while also encrypting that control. Additionally, you must verify and control/limit the connection to and use of external systems and limit the use of portable storage devices on those systems. All UI posted or processed on publicly accessible systems must also be controlled.

Identiv's Thursby Sub Rosa provides a secure mobile solution for CAC/PIV card users that need to access mission-critical sites on-the-go. Sub Rosa has been serving all branches of the Department of Defense (DoD) as well as most non-DoD U.S. government agencies for over 10 years.

It's intuitive interface and easy installation make Sub Rosa perfect for all organizations that need to access U.S. government CUI. Control of UI is the key component in complying with the NIST standard, and Sub Rosa's authentication and encryption method is FIPS 140-2-compliant and is available on the Defense Information Systems Agency (DISA) site. Sub Rosa provides the ability to deliver and receive digital information and access essential services anytime, anywhere, and on any device.

Does Your Organization Need to Comply with NIST 800-172?

Speak to an expert today at **sales@thursby.com** or **+1 817-478-5070.**