

Representative Koford,

Thank you for your prompt response. I understand NIST appears to be a suggestion at a glance, and at the end of my career as the Information Security Officer over Digital Assets at Fidelity Investments, I breathed NIST governance, risk, and compliance like water through a fish gill.

You request independent testing and evidence of Infoton P30 on real systems. The federal compliance architecture makes testing Infoton Prime 30 a federal crime before the first data packet is transmitted (18 U.S.C. 1030, 18 U.S.C. 1343, 31 U.S.C. 3729, FIPS 140-3 Section 4.1). **The pathway to perform the requested independent testing, validation, and maturation of Infoton P30 runs through a formal NIST petition, not the market.**

NIST's own published procedures state that a new FIPS standard is triggered by one of exactly two mechanisms:

- Executive action
- Legislative statute

As the State of Utah has standing to submit a FIPS standard petition, I am asking you to initiate a formal intergovernmental request for the Governor to submit the formal petition to the Secretary of Commerce introduce legislation mandating that NIST create a validation pathway for non-byte-standard architectures.

The higher bar for data center water consumption Governor Cox committed to cannot be achieved without addressing the thermodynamic inefficiency mandated by the NIST byte-standard compliance architecture through the missing 1961 Landauer product requirement.

Federal Landscape

In NIST, current form FIPS 197, Section 3.2 defines the 8-bit byte as the foundational unit of federal cryptographic processing. SP 800-131A lists every approved algorithm with byte-multiple key lengths exclusively. FIPS 140-3 validates that cryptographic modules correctly implement those byte-standard algorithms through the CMVP. A module implementing a non-byte-standard algorithm cannot be submitted for FIPS 140-3 validation because no non-byte-standard algorithm exists in SP 800-131A for it to be validated against. Without exception, every number in *Transitioning the Use of Cryptographic Algorithms and Key Lengths* table is divisible by 8.

Representative Koford, you state "I do not find a law that requires every company to run on an IBM 8-bit architecture or that bars a firm like Infoton from entering the market." You are correct; there is no single statute, but an entire self-reinforcing ecosystem pointing back to

NIST, which is voluntary in name only. Virtually every commercial data center of any scale serves at least one of the following:

1. A federal agency directly
2. A federal contractor,
3. A financial institution under GLBA,
4. A healthcare entity under HIPAA,
5. A cloud provider with FedRAMP authorization.

Each of these relationships imports federal compliance requirements into the facility. To name a few FISMA, FIPS 140-3, FedRAMP, GLBA, SOX, HIPAA, HITECH, America's Water Infrastructure Act, and the Safe Drinking Water Act. Each sector-specific exposure carries individual criminal liability for executives who authorize non-compliant systems. Non-compliant in every case means non-byte-standard, because the byte is the foundational unit of every approved cryptographic algorithm in SP 800-131A, the table every one of these statutes' chains to.

I've taken the time to triage where the NIST requirement lives in each of the major federal regulatory structures which touch data centers and technology. The regulatory capture appears near invisible, until you enter the market.

- FISMA
44 U.S.C. 3554(a)(1)(B) → 40 U.S.C. 11331 → OMB A-130 Appendix I → FIPS 200 Section 1 → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343
- FIPS 140-3
44 U.S.C. 3554 → OMB A-130 → CMVP → ISO/IEC 19790 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343
- FedRAMP
44 U.S.C. 3554 → 40 U.S.C. 11331 → FedRAMP Authorization Act (P.L. 117-263 Section 5921) → OMB Memorandum M-23-22 → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343
- GLBA
15 U.S.C. 6801 → 16 CFR Part 314 → 16 CFR §314.4 → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343
- SOX
15 U.S.C. 7241 → Section 404 → SEC Release 33-8238 → PCAOB AS2201 → COSO 2013 → COBIT → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343 → 18 U.S.C. 1350

- HIPAA
45 CFR Part 164 Subpart C → 45 CFR §164.312(a)(2)(iv) → 45 CFR §164.312(e)(2)(ii) → SP 800-66r2 → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-111 / SP 800-52 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343
- HITECH
42 U.S.C. 17932 → Section 13402 → HHS Interim Final Rule 74 FR 42740 → SP 800-111 (data at rest) → SP 800-52 / SP 800-77 / SP 800-113 (data in motion) → FIPS 140-3 → SP 800-131A (byte-multiple key lengths: AES-128/192/256) → no CMVP validation pathway for non-byte-standard architectures → no breach notification safe harbor → 45 CFR §164.402 → 18 U.S.C. 1030 → 18 U.S.C. 1343
- America's Water Infrastructure Act
33 U.S.C. 300i-2 → SDWA Section 1433 → EPA 817-B-23-001 → NIST CSF → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1001 → 18 U.S.C. 1030 → 18 U.S.C. 1343
- Safe Drinking Water Act
42 U.S.C. 300f → SDWA Section 1459F → P.L. 117-58 → CISA CPGs → SP 800-53 Rev 5 SC-13 → CMVP → FIPS 140-3 → SP 800-131A → 18 U.S.C. 1030 → 18 U.S.C. 1343

Two statutes sit above every sector-specific regulation in this letter and activate upon NIST non-compliance regardless of industry as they require only a computer and an internet connection:

- 18 U.S.C. 1030, Computer Fraud and Abuse Act: operating outside NIST-authorized system parameters exceeds authorized access. Up to 20 years.
- 18 U.S.C. 1343, Wire Fraud: certifying compliance electronically while knowingly operating outside those parameters. Up to 20 years per transmission. Each certification is a separate count.

You can see every sector-specific regulation chains to NIST through implementing guidance, referenced frameworks, or explicit cryptographic requirements. NIST defines the boundary of authorized byte-standard operation. Cross the boundary standard and 18 U.S.C. 1030 applies. Certify electronically that you did not cross that boundary, and 18 U.S.C. 1343 applies. These two regulations are the criminal enforcement architecture that makes NIST non-compliance not a compliance problem but a federal criminal exposure, activated by the same byte-standard requirement that blocks Infoton P30 from every funding pathway and advancement simultaneously.

Every funding pathway I pursued requires NIST compliance as a precondition. The National Science Foundation Small Business Innovation Research require that any technology tested on federal or federally connected infrastructure be built upon my competitors data architecture and meet FIPS 140-3 cryptographic standards before deployment in the research environment. The same applies with Department of Energy in the Office of Cybersecurity Energy Security and Emergency Response, EPA Water Security funding under America's Water Infrastructure Act, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency, and while SBA does not require NIST compliance, Investors do perform due diligence and look for the NIST line item.

Representative Koford, I hope I have provided substantiative evidence that the blocking statute is not in Utah code (although Utah may be able to streamline the Landauer $E=kBT\ln(2)$ requirement to protect water in our region). It is in federal law at FIPS 197 Section 3.2, enforced through SP 800-131A, and activated against any competitor through FISMA, FIPS 140-3, and the CMVP validation process. Submitting concurrent resolution FIPS petition now resolves the data center issue and fulfills two concurrent state mandates simultaneously. The statewide strategic cybersecurity plan required under Utah Code 63A-16-1102, due January 1, 2027, and Governor Cox's Utah Quantum Initiative. A cybersecurity plan written on federal imposed byte-standard assumptions cannot support a quantum computing economy as the byte is not quantum and requires an intermediary layer for our computers today to be compatible with quantum. The layer which the FIPS petition opens the path to.

Ultimately the FIPS petition allows for much needed technological improvements to address Technology's impact on water and the Great Salt Lake, while simultaneously providing a path for real technological advancement in the race for quantum and space.

Thank you for your time reading this message. I've attached a presentation on Technology's impact on Water to add color to the conversation.

January N. Walker

Executive, PISO

ORCID: [0009-0000-6843-2051](https://orcid.org/0009-0000-6843-2051)

<https://infoton.ai/>

Infoton LLC