

The Biden 2023 National Cybersecurity Strategy (NCS) should not be separately assessed in isolation, as its five pillars are based on using the NIST Cybersecurity Framework 2.0 as actually the main implementation tool conceived domestically while serving the U.S. role as champion of a “free, open, and secure” internet against authoritarian models globally. Consequently, it presents immediate transatlantic friction with the EU’s GDPR, the world’s most consequential regulatory apparatus for rights-based cybersecurity. Hence, a complete effectiveness review should also measure not simply domestic risk reduction, either deriving either from compliance with cybersecurity regulatory requirements or nondiscriminatory use of the NIST CSF, but whether the U.S. approach yields fair, rights-affirming outcomes, or reintroduces the very inequalities and cultural hostilities examined earlier about NIST CSF and GDPR.

Bodin et al. (2020, *Journal of Cybersecurity*) and Shires (2023, *Computers & Security*) provide positive conclusions on voluntary or financial incentivized frameworks (like NIST CSF) which produce good uptake by large actors while systematically failing small and medium size entities and individual providers, thus contributing to the digital divide.

Dunn Cavelti & Wenger (2019) and Layton & Elaluf-Calderwood (2020) reveal that even regulatory regimes that seek to achieve regulatory ambition (GDPR) can achieve greater awareness and normative reflexivity with compliance costs weighted towards established technology providers and developers at the expense of startups and emerging technology and digital market entrants.

Marikyan et al (2024) and earlier ethical assessments of the NCS demonstrate that increasing the surveillance powers of agencies (whether grounded in proposed CSF “Detect/Respond” or NCS “disrupt adversaries”, in particular) reduce trust by the public without having enforceable forms of privacy.

Reduction in Measurable Risk Without Concentration of Benefit

The rise and continuing decline in successful high-impact incidents against U.S.. critical infrastructure and citizens (tabulated via CISA with mandatory reporting, disaggregated by the size of the victim).

Similarly with data from EU Member States and GDPR Article 33 breach notifications.

Supporting evidence that SMEs and low-income sectors are not left behind (current data reflects that both NIST CSF and GDPR disproportionately advocate benefitting larger actors).

Equitable Resilience and Economic Effects

Funding for U.S. resilience grants and EU GDPR, including the same percentage invested in startups and SMEs versus large contractors and U.S. Big Tech who work in Europe.

Δ in venture-capital and jobs in the U.S. and EU in the years post-2023 (early indication: GDPR has already cost between 3,000–30,000 jobs in Europe; early regulatory proposals to implement Prioritizing NCS may encourage similar consolidation).

Rights-Respecting Application and Trust (Ethical & Social Pillar)

Independent oversight reports (U.S. Privacy & Civil Liberties Oversight Board & EU European Data Protection Board) were researching the issue of surveillance creep and mission creep.

Longitudinal transatlantic trust surveys (Pew, Eurobarometer): is the public more or less willing to share data in health/crisis situations for societal benefit after five years of NCS + CSF + GDPR?

Presence/absence of mandatory ethics review boards and human-rights impact assessments in their respective regimes.

Global Leadership and Normative Coherence

The extent that U.S. “defend forward” operations and attribution campaigns comply with GDPR territorial scope and charter of fundamental rights.

Measure how many new countries adopt U.S. backed norms versus a rights-based approach reminiscent of the EU. (Expectation is that the current trajectory favors the GDPR model in Sub-Saharan Africa, Latin America and the Indo-Pacific).

As of November 2025, there were substantive signs confirming the patterns observed throughout all prior papers:

Tactical risk reduction is occurring against ransomware and commodity crime primarily for large organizations able to support implementation of NIST CSF Tier 3–4, and GDPR compliance departments are no exceptions.

Small or medium-sized enterprises (SMEs), startups, and the average citizenship is persistently under-protected in either jurisdiction, thereby creating a two-tier digital society.

Public trust is stagnating or declining: sanctioning constant detection and data-sharing (U.S.) and ambiguous fines of approximately €20–50 million (EU) has failed to address the “privacy paradox”; if anything, it has created push back and resentment and work-arounds.

The U.S. and EU are competing rather than converging globally, obliging third countries into a normative splintering, further weakening collective defense.

Conclusion: Partial, Unequal, and Normatively Incoherent success

A rigorous, disaggregated assessment against the four-pillar framework articulated above would deem the Biden 2023 NCS—and by extension its reliance on NIST CSF in tension with the GDPR—as only partially successful. It is successful in disrupting low-end criminal ecosystems and raising corporate hygiene for the already powerful; it is not successful in ensuring equitable risk reduction, maintaining public trust, or presenting a coherent democratic alternative to authoritarian digital models.

Until the United States and European Union transition from voluntary, technocratic (NIST) or punitive, regulatory (GDPR) approaches to binding, audited, rights-by-design frameworks that specifically address rather than perpetuate digital inequality, their flagship strategies for cybersecurity will always remain more performative than transformative. Real success requires measurable protection that extends to the smallest business and least privileged citizen, and does not erode the very rights they claim to be protecting.