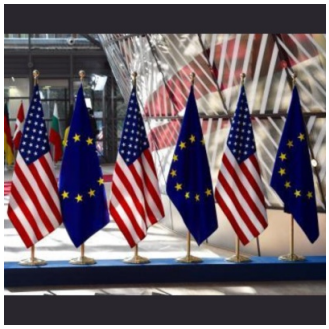
HealthManagement
Promoting Management and Leadership

# DHS & DG CONNECT Launch Cyber Incident Reporting Initiative for Transatlantic Alignment



The first step in this focused initiative includes an analysis of similarities and differences between the recommendations of the DHS Report on Harmonization of Cyber Incident Reporting to the Federal Government and the cybersecurity incident reporting framework under the NIS 2 Directive in the EU.

European Commission's Directorate General for Communications, Networks, Content, and Technology (DG CONNECT) and the US Department of Homeland Security (DHS) announced an initiative to compare cyber incident reporting elements that will inform cyber incident reporting requirements by the US, and European Union (EU) under the NIS 2 Directive. This transatlantic collaboration between the EU and US builds on their efforts to secure their people, critical infrastructure, and businesses against detrimental cyber activities.

The joint report developed by DG CONNECT and DHS, with support from their respective cybersecurity agencies, the European Agency for Cybersecurity (ENISA) and the Cybersecurity and Infrastructure Security Agency (CISA), provides a comparative assessment and factual overview of recommendations from the U.S. Cyber Incident Reporting Council and the 2023 DHS report on *Harmonization of Cyber Incident Reporting to the Federal Government* and EU's *Directive 2022/2555 on measures for high level of cybersecurity across the Union* (NIS2 Directive) by identifying the main similarities and divergences. The findings in this report will help inform DG CONNECT and DHS's approach to evaluating cyber incident reporting processes in the future. The report identifies six main areas for comparative analysis between the DHS's report and the EU's Directive, including: (i) definitions and reporting thresholds, (ii) timelines, triggers and types of cyber incident reporting, (iii) contents of cyber incident reports, (iv) reporting mechanisms, (v) aggregation of incident data, and (vi) public disclosure of cyber incident information.

> Cyber incidents do not recognize borders and multinational companies are often required to report incidents across numerous jurisdictions. We are committed to harmonizing incident reporting rules domestically and with like-minded partners like the European Union whenever feasible. Our approach will allow governmental authorities to get the information they need to provide cyber defense while streamlining the process for victim organizations,

said **Robert Silvers**, DHS Under Secretary for Policy and Chair of the Cyber Incident Reporting Council.

> Across the Atlantic, we seek to work together to compare relevant reporting requirements, including the form or format of information requested seeking ways to minimize the administrative burden on reporting entities,

said **Roberto Viola**, EC Director-General for Communications Networks, Content and Technology

This initiative – which aligns with the 2024 Joint Statement between Secretary of Homeland Security Alejandro N. Mayorkas and European Commissioner for Internal Market Thierry Breton –marks the beginning of a process to align transatlantic cyber incident reporting where feasible. DHS & DG CONNECT invite industry from both the US and EU to share their input and reactions to our joint collaboration and approach to evaluating cyber incident reporting processes.

> This domain is critical as relevant government authorities must have access to information about cyber incidents that impact their citizens or otherwise raise safety and security concerns. Moreover, we recognize that over the next months, both the United States

> and the European Union will continue the work to put mandatory reporting regimes into effect, including by implementing more precise provisions on the process for incident reporting, content of the reports and timelines. It is important to stay connected on these issues and align where possible.

added **Lorena Boix Alonso**, EC Director for Digital Society, Trust and Cybersecurity

> Over the next year our teams plan to continue our cooperation on a more technical level, including by mapping elements such as cybersecurity incident taxonomies, reporting templates, and the content of reports and formats. We will conduct an in-depth crosswalk of the DHS-developed Model Reporting Form against the NIS 2 required contents of reports to identify where there is overlap and disparities in the types of data being requested. As we continue these efforts moving forward, we must remain agile and adapt to the quickly evolving cyber threat landscape as nothing remains static in our digital world for long.

said **Iranga Kahangama**, DHS Assistant Secretary for Cyber, Infrastructure, Risk and Resilience.

The Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), signed into law by President Biden in 2022, established the Cyber Incident Reporting Council (CIRC), led by DHS to "coordinate, deconflict, and harmonize Federal incident reporting requirements, including those issued through regulations." The CIRC, which is chaired by DHS and includes representation from more than 30 agencies, outlined a series of actionable recommendations on how the U.S. Government can streamline and harmonize the reporting of cyber incidents to better protect the nation's critical infrastructure. In 2023, DHS provided a report to Congress including recommendations of the Council entitled *Harmonization of Cyber Incident Reporting to the Federal Government*.

In January 2023, the NIS2 Directive entered into force, giving EU Member States 21 months to transpose it into national law. The NIS2 Directive builds on the requirements of its predecessor, Directive (EU) 2016/1148, concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive), in force since 2016, but it raises the EU common level of ambition on cyber-security, through a wider scope, clearer rules and stronger supervision tools. The NIS2 Directive harmonizes, strengthens, and streamlines security and incident reporting requirements for a larger number of entities, which are critical for the European economy and society.

**Source & Image Credit: DG CONNECT**

Published on : Wed, 20 Mar 2024