CFTC Collection, Concentration, Storage and Securing of Sensitive Information

CFTC TECHNOLOGY ADVISORY COMMITTEE

CYBERSECURITY SUBCOMMITTEE

JERRY PERULLO – CHIEF INFORMATION SECURITY OFFICER, INTERCONTINENTAL EXCHANGE

HUNTER LANDRUM – SENIOR COUNSEL, TWO SIGMA INVESTMENTS

What's The Issue?

Regulated financial institutions - including providers of critical national economic infrastructure - have identified significant risk in the **collection, concentration, storage and securing of highly-sensitive cybersecurity artifacts and sensitive intellectual property** during regulatory examination procedures.

What's The Issue?

- These concerns have been taken up by a variety of United States government oversight groups and buoyed by actual breaches that have occurred at several national regulatory agencies, including the SEC.
- The concern is that much of the data would be extremely useful to an adversary planning a cyber attack against critical economic infrastructure, the CFTC, the markets it regulates, its participants, or the public.
- While useful to support examination activity, this data can be viewed on-site or at mutually-convenient secured facilities and not copied and duplicated where it is no longer under institutional protection.
- Various national and international regulators have taken different stances toward this data collection ranging from an acknowledgement of the danger and agreement to not collect it to insisting on collecting it under cover of regulation and/or recordkeeping requirements, but **currently US regulators such as the CFTC have no clear policies and procedures to aid them in determining when and how sensitive information is securely reviewed.**

What Rule Could Address This Concern?

To better align the CFTC's policies and procedures with its best-in-class practices regarding the limiting of collection of sensitive information, **the CFTC should provide clear, concise and up-to-date guidance on how the CFTC reviews highly-sensitive cybersecurity artifacts and sensitive intellectual property** without compounding risk.

What Analysis Should Inform This Rule?

- Applying a Threat Objective risk analysis to this data theft scenario, the inherent likelihood and impact are well supported by open source intelligence on previous breaches and official recognition of the criticality of national economic infrastructure via executive order, respectively.

- In assessing the residual risk, mitigating controls for both the likelihood and impact fall to the internal security programs of the regulatory agencies themselves.
  - Given the magnified cyber attraction of regulatory bodies if they house highly-sensitive cybersecurity data from multiple critical infrastructures and the perpetual challenges in procuring and maintaining world-class resources to guard these secrets, the residual likelihood and impact - and together the residual risk - remain critically high and demand mitigation.

- Against this backdrop and considering that some sensitive information never loses its value, **the CFTC must codify criteria for permitting on-site review and revise the retention policy for data that is still collected to minimize the amount of information it retains and shift responsibility for legitimate retention requirements to regulated entities.**

Conclusion

With limited value in possessing the data in question, particularly when compared with the commercial risk associated with such possession, **there should be policies and procedures that enshrine the ability for regulated institutions to rely on the CFTC to pursue less invasive tactics before handing certain data over where on-site review is a reasonable substitute.**

Further, relief from recordkeeping and workpaper retention requirements should be explicitly spelled out where strict compliance would otherwise introduce this cybersecurity risk, with alternative measures (such as redacted note-taking) clearly defined as sufficient.