CISA
CYBERSECURITY
ADVISORY
COMMITTEE

REPORT TO THE CISA DIRECTOR

National Cybersecurity Alert System

September 13, 2023

Introduction:

The Deliverable (from CISA 2022 tasking memorandum)

"The CISA Cybersecurity Advisory Committee (CSAC) will produce a report to the Director that will describe the needs, benefits, and operational efficacy of a National Cybersecurity Alert System."

Background:

The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure. As part of its cybersecurity mission, CISA coordinates the execution of US national cyber defense, leading asset response for significant cyber incidents and ensuring that timely and actionable information is shared across federal and nonfederal and private sector partners. This includes analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

> Current State. CISA oversees the National Cyber Awareness System which offers a variety of cyber defense information for users with varied technical expertise. This system produces advisories, alert and situation reports, analysis reports, current activity updates, daily summaries, indicator bulletins, newsletters, recommended practices, a Weekly Analytic Synopsis Product (WASP), weekly digests, and year in review to alert partners of emerging cyber threats, vulnerabilities, and risks. However, these various alerts and advisories do not provide an easily understandable sense of national cyber risk, a characterization of granular changes in the risk environment, and/or continuous coordination among the various federal entities performing similar functions in the present day.
>
> Topic for Study. CISA is interested in understanding the feasibility of an alert system for cyber risk. The goal of this capability would be to provide a clear and simple method to convey the current severity of national cybersecurity risk based upon CISA's all-source analysis of evolving threat activity, such as through a color-coded or numerical "scoring" system. Such a system would complement rather than replace CISA's existing production of alerts and advisories on specific, actionable risks.

Specific questions for the CSAC to address (the "seven questions" from 2022 tasking memorandum):

1. Assess the need for a "National Cybersecurity Alert System" and the specific gap to be addressed.
2. Consider whether CISA is the right agency to provide this type of capability and whether CISA should partner with other federal departments or agencies to be most effective.
3. What should the alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to these cyber threats?
4. Determine the criteria or situations which need to be considered for such a system, to include risk.
5. Identify how CISA could measure the effectiveness of this new capability.
6. Identify a platform or mechanism to ensure there is widespread awareness regarding this capability to ensure it is effectively leveraged.
7. Are there lessons that CISA can leverage from non-cyber national alert systems such as the Federal Emergency Management Agency's Hurricane Alert System and DHS' National Terrorism Advisory.

Additional (amplifying) CISA Guidance from NCAS subcommittee Chair Discussion with CISA Leadership on 12 May 2023:

- CISA is looking for ways to improve the fidelity and sustainability of the current system – one that is more tightly coupled to current conditions and trends.
- The 2022 "Shields up" program combined specific, time-delimited, warnings (ex, "threats are significant and imminent … defenders should lower threshold for sharing *now*") and enduring (general) cyber security guidance (ex, routinely patch, use MFA, enhance segmentation, etc.)
- Emphasis in the proposed national cybersecurity alert system should be on the former.
- CISA expects a small number of recommendations from the Committee.
- The seven framing questions remain valid, but can be expanded as the Committee sees fit.
- A defined role for industry will be important.
- CISA needs a framework and vernacular with which to engage industry.
- A Final Report with recommendations by September 2023 is preferred.

Findings

Question 1: Assess the need for a "National Cybersecurity Alert System" and the specific gap to be addressed.

Discussion:

National Cybersecurity Alert System Contours: There is clearly an appetite for, and a perceived gap in, servicing the expressed interest, on the part of the vast majority of the CSAC NCAS subcommittee and the various private sector interlocutors the subcommittee engaged over the course of the study (see Appendices 1 and 5). Many reflected on the value of CISA's 2022 "Shields Up" campaign, noting that it provided a valuable emphasis on creating awareness of heightened cyber threat, and in providing justification for increased security measures, even if it lacked desired specificity in timing, focus and granularity.

Pulling from lessons identified in the 2009 Homeland Security Advisory Council (HSAC) Task Force report on the Homeland Security Advisory System (see appendix 10), other U.S. Government conditions or alert levels (FPCON, etc.), and inherent differences or limitations in cybersecurity vice other security disciplines, we can define the general contours of a prospective national cybersecurity alert system consistent with CISA's requirements (not accounting for or assessing feasibility under this question). An 'alert' should delineate:

- **Sub-national, Group Specific:** The 2009 HSAC Task Force report made clear that an alert at a national level (without specifics or reference to a target group, region, etc.) is too vague to be useful or actionable. It also noted that in any incident that is significant enough to be a truly national-level issue, an alert system would be useful and likely beaten to the punch by news media.

- **Defined Timeframe of Applicability:** Any "alert" or change in condition would need to define the timeframe in which it is applicable or active. At the end of a timeframe it should be renewed, allowed to expire, or amended.

- **Routinely "Normalized" Baseline:** Any alert system would need to routinely define the assumed "baseline" of threat and risk for a given group for which baseline guidance and short-term, time-limited, measures might be suggested. A sustained threat would thereafter cease to be an alert but incorporated as an element in a baseline "normalized" condition. This would encourage enterprises and business to routinize and optimize security and defense for the specific threat or vulnerability as a matter of standard operating conditions, rather than an unsustainable enhanced readiness/vigilance/increased security posture. Baseline condition would be "no unusual or heightened activity". This is drawn from how FPCON defines its base state and is intended to address a few key concerns raised by the HSAC Task Force in 2009, namely the political issue of reducing the alert level and continuing to maintain heightened or increased risk in an environment where a baseline level of risk is neither defined or assumed as enduring and standard.

- **Condition Set by Likelihood of Targeting or Exploitation:** Existing alert systems inform CISA customers of newly discovered vulnerabilities, indicators of compromise (IOCs), and, on occasion, victim notification. This tactical information is complemented by largely yearly products produced by information sharing and analysis centers (ISACs), the Office of the Director of National Intelligence (ODNI), and CISA on assessment and forecasting of specific threat actor groups.

- **Information at the operational level** is a key missing piece, particularly assessments of threat actor behavior in the day, week, or month timeframe (identification of changes in targeting preferences, new campaigns, etc.)
  - This is a necessary piece in assessing and alerting the likelihood of targeting or exploitation (to detect and mitigate or prevent entirely) for a specific group or at a national level (where applicable) within a defined timeframe.

While the classic definition of "risk" is a function of threat, vulnerability, and consequence, the subcommittee suggests that alerting a specific group that they are likely to be at risk or are targeted (or are already) is the most useful component of system that collects and disseminates risk information. Risk must define the target audience, not merely the threat actor or venue.

Overall Assessment: A national cybersecurity alert system would be a useful service, if executed with rigor, a high threshold for actionability and relevance, and with sufficient supporting intelligence and analysis to be routinely useful. The effort must be given as a primary task to an organization that dedicates full-time resource and focus to the task.

The alert system itself would be useful, no doubt, but its real value would be in the process, capabilities, discipline, and tradecraft that would need to be built in order to field it. Ultimately, the national cybersecurity alert system implicates an enduring question plaguing CISA, and an existential one: What is the business model? What is the value-added and to whom? Key points are captured in the Findings below.

Finding 1: There is a **genuine need** for a national cybersecurity alert system that routinizes the 24/7 consideration and provisioning of cyber alerts and, when possible, guidance to organizations and persons in a position to take action to mitigate identified risk(s) (through a variety of means that include bolstering defense, risk reduction measures, and reducing exposure).

Target groups can be defined using sector, region, size, maturity, and technology for which alerts should:

- Be time-defined or limited (alert levels would then be “normalized”, “extended”, or “reduced”).
- Be based on risk of targeting (or having been targeted) by a threat actor or risk of having an exploited (or likely to be exploited) vulnerability.
- Provide guidance in the initial state change; with additional guidance issued when alert is normalized, extended, or reduced.
- Be informed by and operate alongside existing CISA alerts, advisories, and reports and, where possible, integrate other federal agency products.
- Include a formally defined means to review, alter, or revoke the alert.

Question 2: Consider whether CISA is the right agency to provide this type of capability and whether CISA should partner with other federal departments or agencies to be most effective.

CISA’s implementing statue(s) and relevant executive orders (most notably PPD41) clearly place CISA in the lead role and it would be difficult to argue that any other federal agency is in any better position to take this on. Of note, private sector comments on the national cybersecurity alert system task (see appendix 5) stated that “*The US government has a unique opportunity to synthesize and disseminate threat information that enables disruption of active threats.*” While this aspiration goes beyond a purely national cybersecurity alert system function to imagine a systemic mechanism by which those *alerts* might feed a whole-of-nation effort to *disrupt* cyber threats, it nonetheless highlights the unique position occupied by the government to convene, facilitate, and coordinate nation-wide, cross sector cyber alerts.

CISA's current ad hoc cyber alert and warning system (described as the National Cyber Awareness System) is composed of tactical level "alerts" (notifications of new actions or news), advisories (longer-term reporting of threat campaigns, IOCs, and severe vulnerabilities). The current system is complemented by vulnerability notifications and victim notifications, which are time-consuming, resource intensive, and difficult to scale. That valuable foundation notwithstanding, CISA's current capabilities lack:

- Continuity (a 24/7 focus on warning and alert functions);
- Standardization (use of common, widely understood terminology) of terms like "alert", "advisory", and "bulletin" both in how they are used within one organization (CISA's use has shifted or is amorphous over time) or across the federal government.
- Integration or incorporation of other federal agency alert systems beyond "joint cybersecurity advisories" between CISA, FBI, NSA, and others.
  - Any national cybersecurity alert system would need to track, be aware of, compile, and analytically incorporate federal products into a common risk assessment for an "alert" or state change related to a group.
- Defined timeframe of an alert or advisory (i.e., when it is normalized, or a period of risk has ended).
  - Prescribed revisits of a given warning or alert that provide opportunities to reduce the wear and tear that comes from extended periods of defensive surges that are not based on sustained threats.
  - There is a lack of connectivity and coherence across the various federal and private sector organizations that comprise today's ad hoc alert and warning system.
- Lack of Insight on Cyber Environment, Customer Networks, and "TechStack"
  - Understanding how a threat assessment/likelihood of targeting or exploitation applies to a specific group requires detailed knowledge of the group in question. Currently, CISA has limited or inconsistent/piecemeal information on common technologies, vendors, lines of business, etc. across enterprises within regions, sectors, or sub-sectors— a key data point in trying to determine the scale or pervasiveness of a problem for newly-discovered, severe or critical vulnerabilities.
  - Additionally, beyond what is publicly registered, CISA does not have direct or easily accessible information on ownership of internet selectors like IP addresses— limiting its ability to provide victim notification or indicators and warning to a specific enterprise through threat actor telemetry. CISA does possess administrative subpoena authority to order telecom companies to identify the owner of a specific IP address, but this process is not scalable or particularly useful in developing warnings/notifications of imminent threat.
  - There have been efforts to identify common technologies for certain sectors (e.g., Financial Services), but these have relied on a voluntary process that is uneven and incomplete. There have been other efforts to solicit technical selectors on their IP space for use in I&W and tipping and queuing from critical infrastructure (i.e., Section 9 companies) in a more systematically way, but this has run afoul of perceived legal hurdles and competition with sector specific agencies which are sometimes the exclusive point of engagement for private sector entities.

- Lack of Analytical Capability and Programs - CISA lacks a dedicated standing threat intelligence analysis capability at a scale necessary to support a national cybersecurity alert system (assuming data is even available). Whether such a capability is suffused with sufficient (thus increasing amount of data to compile and assess) or a dearth of analytic capacity (thus requiring making up through inference what can't be determined directly), CISA's current resources, are insufficient in quantity and lacking in specialized areas of expertise (regional threat actors) and analytical tradecraft. CISA could outsource analysis to a third party, like a federally funded research and development center (FFRDC), the Intelligence Community (IC), or another contractor; augment their existing capabilities with in-house contract support specialized and targeted to fulfill skillsets or areas of expertise they currently lack; or forge a coalition of federal and private sector entities that collectively and collaboratively generates needed capacity.

On the matter of which, if any, federal partners CISA should work with to implement a national cybersecurity alert system, the Federal Bureau of Investigation (FBI) is perhaps the closest in possessing capabilities that would make a national cybersecurity alert system viable, by virtue of its geographically distributed network of field offices, an impressive and growing cadre of cyber threat analysts, and a rich feed of relevant threat information (via relationships cultivated by its field network, overseas liaison, and the Internet Crime Complaint Center (IC3) incident reporting system) but it faces limitations similar to those faced by CISA in terms of private sector reporting, available intelligence and the FBI's own ability to publicly post alerts that are sometimes limited by competing priorities of needing to maintain confidentiality for law enforcement operations and/or needing to inform stakeholders to prevent, prepare, or preempt an imminent threat. Appendix 6 ("Overview of U.S. Government Primary Cyber Alerts and Advisories") lists other organizations – not least of which the National Security Agency (NSA)'s Cyber Security Directorate—that are potential candidates for inclusion into a federated approach to implementing a prospective national cybersecurity alert system.

With or without federal partners, CISA would require increases in resourcing, focus, and organization.

Fielding a robust national cybersecurity alert system as articulated above (with tactical-level products and operational-level alerts) that is useful and credible would also require a transformation and refocus of some portion of CISA's core business model— which has largely been defined by assessment of generalized, all-hazards "risk" and tends to be indexed by vulnerability and consequences rather than threat.

In particular, this prospective new model would need to prioritize data collections, analytic tools, analysis capacity and tradecraft, and more targeted, scalable solutions over resource-intensive operations that produce marginal value in data or intelligence terms (incident response, threat hunting, risk and vulnerability assessments, and technical indicator identification), outsource them to sector specific agencies as appropriate, or do away with them entirely.

Finally, while CISA is clearly the most logical choice for leadership of a national cybersecurity alert system capability, the opportunity to leverage the unique capabilities and relationships of the FBI and various Sector Risk Management Agencies (SRMAs) must be seen as both a means to mitigate CISA's current resource deficiencies and to greatly strengthen the capacity and coherence of a US federal effort that serves the collective needs of the private and public sectors for a national cybersecurity alert system .

Finding 2: CISA is the right federal entity to further define and lead the development and implementation of a national cybersecurity alert system.

Finding 3: CISA does not currently possess a framework and supporting organization dedicated to nationwide cyber threat analysis whose goal is to support real-time alerting to defenders. CISA currently lacks analytical capacity and unique, value-added data sources to be able to reliably field a national cybersecurity alert system.

Finding 4: The forthcoming implementation of the 2022 CIRCIA offers CISA a unique data source on current incidents, which can be combined with other government and private information steams to yield a more routine, granular and coherent understanding of threat and/or vulnerability activity.

Finding 5: Additional work in defining SIEs (finding common technologies, lines of business, etc.) and identifying cross-sector enterprises that rely on common or similar TechStacks (i.e. industrial control system (ICS) for utilities, etc.) can be useful in assessing risk and defining groups that may share risk, but the work may be slow and hard to scale.

- **Course of Action #1: No national cybersecurity alert system -** CISA could elect to not pursue a national cybersecurity alert system. To be absolutely clear, a national cybersecurity alert system (as envisioned above) *could* be useful if sufficiently resources, sparingly used and only when credible and actionable, and tailored specific to those most relevant to its contents. But it is not a critical, make-or-break component— it can help optimize, prepare, and make more efficient and targeted periods of enhances security procedures. Existing CISA tactical alerts, IOCs, advisories (campaign-level), and vulnerabilities provide a steady stream of actionable content to enterprises. Though lacking in context and intuitive method of quickly assessing its relevance, it is a baseline function that can help enterprises that are paying attention.

- Course of Action #2: National cybersecurity alert system-lite - CISA could develop a national cybersecurity alert system that only follows *some* of the criteria or key dimensions outlined above. It could, for instance, focus on issuing alerts and assessments reactively, only in instances where a campaign has been identified and disclosed (usually through advisories) or a particular severe vulnerability has been identified. What is most meaningful here is being able to tailor the alert and its distribution to particular groups or sets— that would still need to be maintained. However, shifting from predictive/forecasting to reactive alleviates the need for greater analytical capacity and larger quantities of data and threat intelligence. General alerts for specified groups would lack the total context of a full national cybersecurity alert system but would still provide some indication of relevance and priority absent in the current alerting system.

- Course of Action #3: CISA-FBI national cybersecurity alert system - CISA could partner with the FBI in fielding this capability; it is standard procedure for more operational-level or strategic "advisories" (usually outlining and disclosing an adversary campaign with associated IOCs) to be multi-seal, collaborative, and consensus documents jointly issued by multiple US agencies. CISA and FBI have been the core partners in these advisories (and have the longest-standing collaboration). A national cybersecurity alert system would be a natural evolution in this partnership. The challenges are many but, workable. Lack of communication between field offices and FBI HQ and competing priorities as noted above continue to plague this collaboration and would likely do so under a joint national cybersecurity alert system. Additionally, the lack of routine sharing of or access to each agency's raw data (particularly in FBI's case) puts limits on the extent of analytical collaboration. CISA and the FBI would have to work out decision-making and authority for alert issuance. It is likely that the contours, thresholds, "groups", distribution channel, and other key dimensions of a national cybersecurity alert system would need to be shaped by FBI as a condition of their participation and partnership. While this cedes some control from CISA in the design and stewardship of the capability, it is a worthy tradeoff for greater leverage of FBI threat information, analytical resources, and relationships (especially the cyber focused staffs deployed across its national and international offices).

- Course of Action #4: Future national cybersecurity alert system - The passing of the CIRCIA provides CISA a critical and unique capability, namely indicative if not comprehensive threat intelligence and incident-related data on an enduring basis (for critical infrastructure). This fills a much-needed gap for the agency and resolves its lack of a unique, scalable source of threat intelligence. CIRCIA is still in its rulemaking process, affording CISA ample time to both take full advantage of the information CIRCIA can offer and build-out capacity and capability necessary to make a national cybersecurity alert system viable, useful, and credible. In particular, CISA could build out its analysis capacity; develop or procure new analytical tools in a modernized infrastructure; develop qualitative metrics and threshold for a national cybersecurity alert system; and define workable, scalable ways to identify common technologies/interdependencies among sectors/regions that are useful in assessing scope of vulnerability impact. This course of action is not mutually exclusive with partnering with the FBI and, in fact, affords both agencies more time to work out kinks in governance, framework, joint systems, and information sharing— issues that are key policy and procedural questions in CISA's implementation of CIRCIA.

Question 3: What should the alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to these cyber threats?

Discussion:

Discussions with private sector cyber security professionals (see appendix 5) and with Israeli and UK CISA-counterpart organizations (Appendices 3 and 4) highlighted a compelling statement of need for such an alert system. The private sector discussants noted that the US government has a unique opportunity to synthesize and disseminate threat information that enables disruption of active threats. Their comments framed the constituent components of a useful cyber alert system as:

- The alert system should:
  - Serve ONLY for the timely dissemination of urgent and actionable alerts that enable recipients to anticipate and prepare for specific cyber threats.
  - Optimize for cyber incidents that are ongoing or have recently happened and continue to produce damage, vulnerability, and potential harm.
  - Optimize the reporting pipeline to incentivize and accommodate high-fidelity, high-value cyber incident reporting sources. Speed and action ability will be an essential components.
- More specifically, the alerting system should emphasize creating mechanisms for:
  - Directly reporting to victims or their security vendors that can take actions.
  - Determining relevant **actioning stakeholders** (organizations or people that can take actions to mitigate harm or categorically disable attacker capabilities).
  - Inform the security practitioners at relevant verticals or affected organizations.
  - Use global broadcasting ability ONLY when absolutely necessary.
  - Define a clear value adding function that naturally incentivizes operators to involve CISA in order to reach a favorable outcome.
  - Focus on enabling action(s) that prevents, interdicts and/or disrupts threats.

The elements included in a given alert would vary depending on the imminence, focus, and scope of the given threat or vulnerability. Appendix 6 describes a Possible Framework for Cybersecurity Information by type and level, but any alert should include the elements identified above by the private sector security professionals engaged during this study, any relevant guidance on actions that may mitigate or prevent the threat identified by the alert, and a mechanism for reviewing the alert over time to adjust and/or terminate the alert based on changing conditions.

A national cybersecurity alert system would then seek to (using CISA's existing products and data), identify instances where a specific group is at heightened or imminent risk that they are or have been targeted by a threat actor group or have a known/discovered vulnerability that will be or has been exploited.

- **Feasibility Considerations:** The "national cybersecurity alert system contours" discussion under Question 1 of this report was generated assuming that CISA has - or can attain - capabilities necessary to be able to routinely issue relevant, actionable alerts and has sufficient data/intelligence to tailor it to a specific group and assess likelihood of targeting or exploitation. However, we need to determine the feasibility of CISA actually being able to field this capability. In this regard, CISA faces a series of considerable challenges and limitations, not only in the information available to it, but in its own analytical capacity, ability to share or incorporate data from external sources, and knowledge of technical and functional environment necessary to identify when a threat or vulnerability may be most applicable to a specific, tailored group.
- **Inherent Limitations of Cyber Threat Intelligence -** As opposed to counterterrorism, natural hazards, or other conventional domains, cybersecurity is critically limited in that it rarely has *direct knowledge* of the threat actor (i.e. direct surveillance or intelligence on adversary operations and decision-making) at a tactical level. Most knowledge is derived from technical information collected from incidents. Understanding the context of any one incident (and whether it is indicative of change/consistency in pattern of behavior or an anomalous data point) takes time through incidental discovery, time in assessing and linking multiple incidents, tying to a threat actor, and, finally, assessing or forecasting the significant of the behavior in the context of threat actor objectives, patterns of behavior, etc. This means that threat intelligence often lacks context, operates on a significant time delay (often but not always), and does not benefit compared to other security disciplines from the US's existing strengths in foreign intelligence collection. A compounding factor is that much of the data by which to make informed assessments are held by disparate cybersecurity, incident response, or threat intelligence firms— who have little incentive to share information that could diminish their competitive advantage relevant to their competitors.

- **Key Limitations on US Government Threat Intelligence -** The most obvious limitation on US government threat intelligence is the inability to deploy sensors domestically at scale— either to monitor general internet traffic or monitor the networks of specific enterprises. CISA has fielded some prototype capability through voluntary agreements, but it does not appear this program has been made a principal program and scaled to a level where necessary network effects can make it viable. Further, in instances where the government does place sensors on domestic networks (e.g., FBI sensors on compromised networks, Department of Energy (DOE)'s Cybersecurity Risk Information Sharing Program (CRISP)) the information is siloed and not routinely shared. Existing programs like Einstein-3A and Enhanced Cybersecurity Services have faced increasing ineffectiveness due to technological change (encrypted network traffic, move to cloud hosting by US government, etc.) or dearth of collection of classified indicators.
- **Ineffective or Absent Public-Private Threat Sharing -** It is unlikely the US government can persuade (or force) cybersecurity, or threat intelligence companies to share information they consider a trade secret. Previous attempts to remove barriers to sharing (e.g., prohibition on regulatory use, limited liability protection, etc.) have not been effective in encouraging sharing at scale. Programs like Automated Indicator Sharing (AIS) have seen less than expected participation by private sector partners and lack the context the private sector needs to appropriately determine the relevance, priority, and actionability of any given data point. It is unlikely this is a solvable problem in the near-term; CISA's focus appears to be in established trusted communications channels between targeted partners to coordinated operations and information person-to-person; rather than designing and fielding a technological medium for automatic tactical threat sharing and collaborative assessment (as reflected CISA's arguments against the Congressional recommendation in legislative year 2022 for a formally constituted *Joint Collaborative Environment*).

Defining target audiences is perhaps the most difficult portion of a national cybersecurity alert system implementation.

Alerts should be relevant and tailored to a specific group and, indeed, the accuracy and usefulness of any assessment is helped considerably by how focused/narrow the group being evaluated is. If the audience is too large, the benefits of an alert are diluted, lack precision, and lose relevance and influence over time. A sector-based grouping system is useful, intuitive, and has ready-made distribution channels via ISACs; however, it does not account for the incredible disparity in security maturity across most sectors— the size and maturity of an organization being a significant factor in targeting either intentionally or through opportunistic vectors.

CISA may find it advantageous to use one or more grouping definitions (that can be cross-cutting) that can serve to focus the alert, define to whom it applies, and guide targeted distribution. Risk would then need to be assessed by the groupings together rather than individually. There are a few key grouping types that should be used (though there are many, these are selected for their intuitiveness and simplicity):

- **Sector or Sub-sector -** The most identifiable grouping, with a ready-made distribution network, and routine assessment of group-wide risks and threats. It is not enough on its own, however, as even within critical infrastructure (CI) sectors, there are a number of other significant factors that weigh into a threat actor's targeting preferences. Additional detail/distinctions need to be made.
- **Criticality** - Sector or sub-sector presumes critical infrastructure, but an additional field to specify critical is useful when an alert only applies to SIEs/SICIs or in instances where an alert may be more general and apply to all enterprises irrespective of their specific criticality (i.e. there is no specific sector or sub-sector to be defined).
- **Region or Locality** - Likely a rarely used field, it may nevertheless crop up from time-to-time, particularly with criminal actors that have a regional preference or areas where a sector or sub-sector is concentrated (DC and Government, New York and financial, etc.), or activist/localized campaigns targeting a specific municipality.
- **Technology "Clade"** - CISA has done some general definition to define enterprises by their technology stack, making a distinction with ICS alerts versus more general IT-focused ones. There may be more to be done here, to identify groupings of businesses that share network architecture, equipment and device type, and services in common - and thus have a similar risk profile re: vulnerability. ICS/OT is a good distinction, one that walks a fine line between being broad enough to loop in a significant portion, but not too broad as to dilute relevance of any given alert. It is also intuitive. Something like "Microsoft Office users" maybe too narrow. Other clades could

include Home or Small Enterprise (COTs devices, few firewalls, no on-premises, personal device use), Development Environments (software developers, etc.). More research is needed on this, but the subcommittee believes that groups sharing common "stacks" can be identified at a similar scope and would be a useful distinction to make.

- **Mission or Business Activity** - It may be worth having an additional distinction on mission or business activity. For example, for Chinese threat actors pursuing China's research and development (R&D), science and technology (S&T), and economic development goals through IP theft sending alerts by defined by sectors (Academia, Defense Industrial Base, etc.) may be too broad to be useful and is not the principal way the actors would define their target set. It would be by mission or business activity. "Quantum Information Science", "Artificial Intelligence Research", "Stealth and Meta-material Development", would be more useful and better aligns to the commonality between different enterprises that is the reason for targeting. Similarly, distinctions such as "Utilities" are inherently cross-cutting and are more accurate and efficient distinction for certain types of threat actor targeting preferences than simply saying "Electric", "Water", etc. There needs to be some research on a mutually exclusive, comprehensively exhaustive taxonomy (for consistency and to ensure differentiation/distinction with sector and sub-sector groupings) but that's beyond the scope of the study.

Question 4: Determine the criteria or situations which need to be considered for such a system, to include risk.

Regarding possible Levels and Risks Calculation - There was general consensus among public respondents to this study, and from HSAC Task Force members in its 2009 study, that any alert system should hew to the use of specific language and avoid using colors or other broad ‘labels’, both because it does not capture the full context/message that needs to be conveyed and it draws and unhelpful and unfortunate connection to the poorly regarded former terrorism alert system.

- The current National Terrorism Advisory System (NTAS) uses simple descriptors (heightened, elevated, etc.) rather than colors or numbers.

- CISA *could* attempt to define some quantitative method to define risk (or likelihood) of targeting within a defined timeframe for a given group, but we would suggest that there are too many unknown variables at play to arrive at a satisfying and consistent method that would have enduring credibility. A more qualitative method may be more useful and efficient and less subject to false certitude that can lead to overconfidence and critical errors.

- Existing frameworks to assess the severity of newly discovered vulnerabilities are extremely useful as a data point, but they do not speak to a vulnerability's pervasiveness within a given group or the likelihood and degree it will or has been exploited by threat actors. That additional information needs to be included and should be assessed qualitatively.

- The National Cyber Incident Severity Schema (NCISS) and other similar frameworks for evaluating severity or impact of an incident, while great tools for emergency management and incident response, are not applicable, here. They only speak to the severity and significance of an incident after-the-fact, not the likelihood of targeting of a specific group or exploitation of a vulnerability.

Regarding Content and Distribution - Similar to the NTAS, the national cybersecurity alert system should take a two-channel approach. This includes: 1) a short, publicly-posted "blurb" or "card" that summarizes the key details of the alert or heightened condition, who it is relevant to, and other top-level relevant factors; for National Terrorist Alerts there is usually an attachment or document with additional guidance or detail *for public consumption;* and 2) direct notification or distribution to participating members of the identified, relevant group, accompanied with additional detail, guidance, etc. that were not (or could not) be included in public versions.

Regarding Threshold - CISA has to maintain a delicate balance. Given the amount of activity in cyberspace, it would be ideal if CISA had sufficient data to be able to generate these insights *only* in instances where a threat or vulnerability is truly widespread, has a high likelihood, and contains actionable information. Without a lot of data to be able to achieve this, there could be a tendency to reduce the threshold to increase the number of alerts (resulting in scope or "threshold drift"). This would lead to a downward-trending dynamic where alerts are diluted and are not meaningfully distinct from the tactical-level alerts CISA already generates. To engineer against this natural dynamic, the threshold decision-making authority should be placed at a high-level (CISA Director, Deputy Director, etc.) and should be evaluated against a set of rigorous qualitative metrics and benchmarks to be considered and actioned.

Finding 6: Alerts must be specific, targeted, actionable and subject to periodic review to ensure they remain current or are adjusted and/or terminated in a timely manner.

Regardless of the choice made for or against tiering, the CISA national cybersecurity alert system Team should rigorously consult with Sector Coordinating Councils, federal partners, and foreign counterparts on the characteristics of the proposed national cybersecurity alert system.

Question 5: Identify how CISA could measure the effectiveness of this new capability.

The mere **existence** of credible alerts, actionable information and attendant guidance on how recipients can better prevent or respond to cyber threat is a measure of effectiveness in and of itself. **Coherence** of federal efforts to solicit, synthesize, and disseminate cyber alerts is an important secondary measure that will deliver needed efficiency and optimal results in a system that is inherently heterogeneous in needs and capabilities.

Question 6: Identify a platform or mechanism to ensure there is widespread awareness regarding this capability to ensure it is effectively leveraged.

Identifying organizational responsibility (within the federal government) and the role of nonfederal stakeholders (private sector and CISA international counterparts) will be as important as identifying the platform, mechanism, or process.

Finding 7: The lack of an agreed-upon framework to assess risk across a defined group (e.g., sector, region, size, maturity, and technology "clade") under such a national cybersecurity alert system is a significant barrier to implementation. Existing systems like the National Cyber Incident Scoring System (NCISS) or National Cyber Incident Severity Schema are useful starting points but are intended to assess severity of an *incident* rather than risk of a particular threat actor or vulnerability's impact on a specified group and would need to be modified and adapted to generate a new alerting level schema.

Question 7: Are there lessons that CISA can leverage from non-cyber national alert systems such as the Federal Emergency Management Agency's Hurricane Alert System and DHS' National Terrorism Advisory System

After examining both the frameworks for the National Weather Alert System and the US Terrorism Alert System (a more detailed assessment can be found in appendices 8 and 9 of this report), each are intuitively appealing, yet perceived similarities are offset by distinct differences in the nature of both the threat and its impact. As noted in the discussion under Question 1 of this report, lessons identified in the HSAC Task Force report on the NTAS in 2009, other US government conditions or alert levels (FPCON, etc.), and inherent differences or limitations in cybersecurity vice other security disciplines, can help define the general contours of a prospective national cybersecurity alert system consistent with CISA's requirements (not accounting for or assessing feasibility under this question).

Finding 8: Previous experience with terrorism alerts suggests that the viability of any national cybersecurity alert system requiring nonfederal entities to provide or act upon information that affects their operating efficiency and/or liability to shareholders, regulators and customers will depend on a mix of incentives and liability shields to encourage private sector participation in generation of information underpinning alerts.

Recommendations:

- CISA should assign the task of developing a national cybersecurity alert system to a dedicated team ("CISA national cybersecurity alert system Team" equipped with the authority and resources needed to define, implement, and lead an operational national cybersecurity alert system.
    - In implementing this action, CISA should avoid simply utilizing existing distribution lists for alerts and instead take the opportunity to enhance its understanding of the intended customer set - filling in key gaps in its knowledge of the cyber environment. In any "sign up" campaign for the national cybersecurity alert system (not the tactical level alerts, advisories, and guidance, but the direct-to-group operational-level change in their risk condition), CISA should include a questionnaire with basic questions on sector, sub-sector, region, and business activity (group distinctions above) by which it can automatically tailor and distribute alerts in the future. Another consideration is limiting enterprises or organizations (at the lowest discrete legal entity-level) to one account (with multiple distribution emails/points of contact) to avoid conflicting or erroneous information.
- The CISA national cybersecurity alert system Team should initiate its work by identifying and working with stakeholders to define the purpose(s), formats, target groups, and measures of effectiveness for cyber alerts.
- The CISA national cybersecurity alert system Team should develop and implement a federated model for the national cybersecurity alert system that leverages authorities, capabilities, and infrastructure across the federal government and its counterparts in the private sector – the Committee offers several courses of action here but strongly recommends one that partners with the FBI organization leading threat response under PPD41 and with sector specific agencies leading sector cyber engagement.
    - In conjunction with ODNI and NSA, the CISA national cybersecurity alert system Team should review processes and procedures specific to the U.S. Intelligence Community CRITIC process (IC Directive 190) to include the newly established Intelligence Community Cyber Threat Alert, to determine whether that process is relevant or should be integrated into the national cybersecurity alert system.
    - In conjunction with FBI and other relevant partners identified under PPD41, the CISA national cybersecurity alert system Team should consider and implement one or some combination of the following four distinguished courses of action (COAs). Each one makes a tradeoff on key dimensions of an optimal national cybersecurity alert system: need, quality, control, and timeframe. CISA should follow COA 3 with a view to enhance that approach using COA 4 as time and circumstances allow.
- The national cybersecurity alert system should consider a tiered release strategy that provides most timely and granular information to those with largest equity and ability to action the information-in-question on behalf of the broadest population of downstream users. Ring 0 covers warnings that are imminent and specific. A possible tiering strategy (the timeliness requirements are loosened, and the audience expands as the tier number increases):
    - Ring 0: Targeted entities for <u>imminent</u> warnings that are specific and/or significant in impact (concurrent with cc: to affected SRMAs).
    - Ring 1: Affected entities for <u>non-imminent</u> or <u>non-specific</u> threats (e.g., multiple/cross-sector threats or a technology in wide use).
    - Ring 2: Relevant SRMAs and ISACs for sector specific alerts, warnings and/or guidance.
    - Establish process to coordinate development and release of alerts, warnings, and guidance to FBI's National Cyber Investigative Joint Task Force, NSA's Cybersecurity Collaboration Center, SRMA's, and ISACs.
    - Provisions should be made for delegated authority to NSA, FBI, SRMAs, and ISACs that ensures the right alignment of efficiency and coherence.
    - Getting actionable alerts from numerous entities might undermine the actionable nature of seemingly contradictory alerts.

  - Consideration should be made whether it is better for there to be only ONE entity that sends out the Alerts– in particular Ring 0 alerts. NOTE: The Israeli model centralizes responsibility for cross-cutting and critical alerts to the central authority.

- The CISA national cybersecurity alert system Team should build on existing CISA monitoring processes and associated National Cyber Incident Scoring System (NCISS) to add *warning*, *alert*, and *guidance* functions (that yield the so-called national cybersecurity alert system) that ensure this knowledge is leveraged for the benefit of cyber users. Definition of these terms follow:
  - Warning: information reflecting expected imminent threats (a special case of alert based on significant imminence and impact)
  - Alerts: information reflecting periods of increased threats that lack specificity in time or affected entities
  - Guidance: information reflecting best practices in prevention and/or remediation
  - All the while ensuring that the national cybersecurity alert system remains connected and is wholly aligned to the National Cyber Incident Response Plan as it is built out from the extant ad hoc warning system.
- The CISA Director should task the CISA General Counsel (with assistance of the Office of the National Cyber Director chaired cyber lawyers council) to examine and recommend a legal framework, incentives, and protections connected to sharing and acting on cyber threat information.

Conclusion:

There is strong value of a national cybersecurity alert system led by CISA which would leverage and connect the work currently done by various federal agencies, departments and private sector entities. A national cybersecurity alert system should complement rather than replace the continuous exchange of information on cyber risk trends and best practices.

The prospective national cybersecurity alert system should provide specific, actionable and time sensitive information to cyber defenders on imminent cyber risk. As described in further detail in this report, CISA should build on CIRCIA implementation to harness the prospective collaboration between federal agencies to meld CIRCIA information with other streams of threat and vulnerability information. This would feed an alert system led and executed by CISA and relevant agencies possessing unique capabilities and relationships.

Appendices:

Appendix 1: Methodology employed to conduct the national cybersecurity alert system Study

Appendix 2: List of contributors to this report

Appendix 3: Summary notes of subcommittee engagement with Israel Cyber Directorate

Appendix 4: Summary notes of subcommittee engagement with UK National Cyber Security Centre

Appendix 5: Summary of comments and recommendations from the Ploessel CISO engagement

Appendix 6: Overview of U.S. Government Primary Cyber Alerts and Advisories

Appendix 7: Possible Framework for Cybersecurity Information by Type and Level

Appendix 8: Parallels and Differences Between a prospective national cybersecurity alert system and the extant US National Weather Alert System

Appendix 9: Parallels and Differences between a prospective national cybersecurity alert system and the extant US Cyber Terrorist Alert System

Appendix 10: Additional Resources

Appendix 1: Methodology employed to conduct the national cybersecurity alert system study

CSAC established a subcommittee to undertake a broad engagement and iterative development of findings and recommendations that included outreach to the private sector, international counterparts, and federal agencies and departments involved in the assimilation and dissemination of [ad hoc] cybersecurity alerts.

External Outreach (across the period late 2022 to August 2023):

- DHS/CISA to provide specific scenarios that give shape and form of what CISA is looking for
- Explored lessons from the U.S. Terrorism Alert System; and National Weather System (e.g., Hurricane Alerts)
- UK National Cyber Security Center and former senior leaders (Ciaran Martin, Paul Chichester, David Omand)
- Israel National Cyber Center (Gaby Portnoy, Aviram Atzaba, and staff)
- US Office of the National Cyber Director (Brian Scott)
- US Federal CISO and CIO (Chris DeRusha, Clare Martorano)
- The National Security Agency Cyber Security Directorate (Morgan Adamski)
- FBI Assistant Director for Cyber (Bryan Vorndran)
- Canadian Security Establishment (Shelly Bruce; Rajiv Gupta)
- US government cyber lawyers group to explore liability shield or safe harbor for good faith efforts based on warning (Paul Tiao)

Appendix 2: List of contributors to this report

The following NCAS subcommittee members participated in the study and recommendations documented in this report

Subcommittee Members:

- Chris Inglis, Subcommittee Chair, Former National Cyber Director
- Jennifer Buckner, Mastercard
- Kathryn Condello, Lumen Technologies
- Niloofar Razi Howe, Tenable
- Kevin Mandia, Mandiant
- Jeff Moss, DEF CON Communications
- Suzanne Spaulding, Center for Strategic and International Studies
- Alex Stamos, Krebs Stamos Group
- Patrick Turchick, Johnson & Johnson

Interviews were conducted with:

- Israel Cyber Security Center
- United Kingdom National Cyber Security Centre (NCSC)
- Ad hoc group of private sector CISOs facilitated by JCDC participant, Matt Ploessel
- The Office of the National Cyber Director
- The FBI Assistant Deputy Director for Cyber (Bryan Vorndran)

Appendix 3: Summary notes from Interview with Israel's Cyber Directorate, 20 July 2023

Questions teed up by the US NCAS subcommittee to frame the discussion:

- What should a cybersecurity alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to cyber threats?
- What criteria or situations should be considered for such a system, to include risk?
- How would the effectiveness of this new capability be measured?
- Is there a platform or mechanism that would ensure there is widespread awareness regarding this new capability, to ensure it is effectively leveraged?
- What are some lessons learned from other, non-cyber national alert systems?

Israeli team Comments:

- Israel has had an alert system for several years and is currently revamping it based on accumulated experience.
- The system has often been overwhelmed with too many alerts that are poorly distinguished from one another and lack operational context.
- Solution:
    - Prioritization based on the criticality of the impact of a given threat;
    - Crisper role assignment to central and distributed government authorities;
    - Stronger integration of process and operations.
- The Israeli system provides 3 kinds of alerts:
    - Critical function alerts to internal Israeli entities;
    - Alerts (and guidance/assistance) to private sector entities provided by sector leads;
    - Alerts to international partners.
- Alerts should be: actionable; convenient to receive and clear in their meaning;
    - Emphasis: Actionable information is vital.
- Coherence across the multiple participants in an *alert* system is vital (for Israel, the central authority is equivalent to CISA; sector agencies are equivalent to US counterparts; the private sector collaborates more closely with both).
    - The central authority focuses on critical functions (which cut across stove piped sectors) with bias to provision actionable alerts to the most critical functions.
    - Sector agencies focus on their respective sectors with a bias to provision continuous assistance and guidance and provide regulatory oversight.
- Physical integration of the various federal entities participating in this system is important to create the seamless integration of disparity government capabilities, authorities and perspectives.
- One must recognize that the various critical sectors differ significantly in maturity and ability – prioritize your efforts accordingly.

Appendix 4: Summary notes from interview with UK National Cyber Security Centre (NCSC), 1 August 2023

Summary of discussion:

- Inglis led off with a [very] brief summary of the task being worked by the subcommittee and reprised the 4 framing questions sent in advance to the UK discussants:
  - What should a cybersecurity alert system highlight? What does a cybersecurity alert capability need to include to facilitate industries', as well as government's, response to cyber threats?
  - What criteria or situations should be considered for such a system, to include risk?
  - How would the effectiveness of this new capability be measured?
  - Is there a platform or mechanism that would ensure there is widespread awareness regarding this new capability, to ensure it is effectively leveraged?

General [opening] remarks by UK colleagues:

- UK does not have a threat alert system per se; though they have issued NCSC notifications for "heightened threat" (e.g., on the eve of the Russo-Ukraine war) and recommendations for increased preparation during special events (e.g., the London Olympics, coronation, etc.).
- There has been interest in a terrorism-like alert system with a graded scale.
- The challenge is that the terrorism alert system comes with legal and operational implications for each level which are difficult to define for cyber.
- The challenge for cyber is attaching objective legal and action-oriented measures to each of the prospective levels we might employ in such a scheme.
- As a consequence, the UK system is not threat led; (e.g., No shields up) but they do "put a general awareness and preparation wrapper around specific real-world events" (Coronation, Olympics, etc.).
- UK occasionally put out episodic alerts and advisories for specific clusters of providers, operators, and/or sectors. Often based on specific, classified, information. These ad hoc alerts are supported by a monthly session among government representatives of the various sectors served by HMG who, in turn, remain in continuous contact with their private sector counterparts .... The point here is that there is a continuous flow of information, vice episodic threat alerts.
- <u>KEY POINT</u>: UK system is anticipatory and continuous; Emphasis is on preparation vice reaction as the predominant behavior; the UK finds the U.S. goal for a national cybersecurity alert system appealing but the UK does not have a scheme to introduce it with objective, repeatable standards, legal framing, and attendant actions for each.
- The UK recommends the US speak to the Norwegians who have a system called "Cyber Pulse" that seems to capture much of what the US is seeking to install.

US Participant Questions and Comments

- <u>Comment</u>: "Where we [the US and UK combined] are, is not bad ... the example of the terrorism alert system is far less helpful than we originally imagined it might be (it is unduly reactive, episodic and focused on the negatives of threat vice the positives of resilience borne of preparation and continuous consultation that addresses and precludes unnecessary risk)".
  - Both countries issue advisories and alerts when we discover a threat (often based on recently discovered technology flaws or a significant rise in threat actor action).
  - The biggest challenge is how you ratchet back down – avoiding the desire to capture the nuance of the situation with a color or a phrase (intuitively appealing though far less useful in practical application).

- <u>Comment</u>: "Preparation seems to be the preferred behavior, vice response".

- <u>Question</u>: "Which messaging is more impactful?"
  - <u>UK response</u>: Specificity is the key – describing the nature of the threat <u>and</u> what the impact would be if

it lands; very important to be specific in describing the nature of the problem and whatever actions may be appropriate to deal with it.

- The discussion concluded at the end of the prescribed 30 minutes allocated. The UK discussants will pass contact information for the Norwegians (their *cyber pulse* system) and any additional comments they may have on the questions posed by US discussants.

Appendix 5: Summary notes from engagement of Private Sector CISO Council

The following was obtained in various conversations with representative – but not exhaustively so – CISOs and JCDC Participants

In general, the private sector seeks greater action ability in disseminated information; greater proactivity in government actions to mobilize disparate authorities to crowd source and interdict cyber threats; and greater coherence in roles and responsibilities of government entities that provide alerts and guidance. *(Detailed, informal, recommendations are under development and can be provided at a later date)*

Specific private sector comments from enterprise security professionals relevant to the creation of a national cybersecurity alert system *are:*

- The alert system should serve ONLY for the timely dissemination of urgent and actionable alerts that enable recipients to anticipate and prepare for specific cyber threats.
- The alerting system should optimize the alerting process and follow on actions to notable cyber incidents that are ongoing or have recently happened and continue to produce damage, vulnerability, and potential harm.
- Optimize the reporting pipeline to incentivize and accommodate high-fidelity, high-value cyber incident reporting sources. Remove friction and promote favorable outcomes. More specifically:
- Emphasize creating mechanism for:
    - Directly reporting to victims or their security vendors that can take actions.
    - Determining relevant **actioning stakeholders** (organizations or people that can take actions to mitigate harm or categorically disable attacker capabilities).
    - Inform the security practitioners at relevant verticals or affected organizations.
    - Use global broadcasting ability ONLY when absolutely necessary.
    - Define a clear value adding function that naturally incentivizes operators to involve CISA in order to reach a favorable outcome.
    - While alerts are inherently and intuitively valuable, the focus must be to enable action that prevents, interdicts and/or disrupts threats.
    - The US government has a unique opportunity to synthesize and disseminate threat information that enables disruption of active threats.

Appendix 6: Overview of U.S. Government Primary Cyber Alerts and Advisories

Background: The complex information sharing and stakeholder relationships among federal agencies have resulted in redundancies and gaps in the presentation and availability of useful cybersecurity products. This section aims to list and describe key products produced by key federal agencies.

Cybersecurity and Infrastructure Security Agency (CISA): CISA leads the nation's efforts to protect and strengthen critical infrastructure against cyber threats. Their focus is on risk assessment, incident response, and information sharing. The following are some of their key cyber alert and advisory products:

- **Security Bulletins:** Comprehensive analyses of emerging threats, trends, and best practices for cybersecurity professionals.
- **Alerts:** Timely notifications addressing significant cyber threats, vulnerabilities, and incidents.
- **Cybersecurity Advisories:** Detailed guidance and recommended actions to mitigate specific cyber risks and vulnerabilities.

Federal Bureau of Investigation (FBI): The FBI plays a crucial role in investigating and combating cyber threats. More specifically, the FBI's role under PPD41 identifies them as a key partner in ensuring that alerts are fully leveraged to enable threat response. Their approach includes proactive intelligence gathering and collaboration with law enforcement agencies. The following are some of their key cyber alert and advisory products:

- **Flash Alerts:** Immediate notifications providing time-sensitive information on significant cyber threats and recommended actions.
- **Private Industry Notifications:** Targeted alerts and information sharing with private sector partners to address emerging cyber threats.
- **Threat Intelligence Bulletins:** Timely bulletins providing insights into emerging cyber threats and recommended actions.
- **Public Service Announcements (PSAs):** Publicly available announcements highlighting significant cyber threats and providing mitigation strategies.
- **Security Advisories:** Detailed advisories on specific vulnerabilities or threats, including mitigation recommendations.

National Security Agency (NSA): The NSA plays a vital role in the nation's cybersecurity by providing intelligence and expertise to protect national security systems. Their products emphasize advanced techniques and insights. The following are some of their key cyber alert and advisory products:

- **Cybersecurity Information Sheets (CSIS):** Brief, practical guidance on critical cybersecurity topics and emerging threats.
- **Cybersecurity Technical Reports:** In-depth reports providing analysis, insights, and technical details on advanced cyber threats and vulnerabilities.
- **Cybersecurity Advisories:** Actionable advisories offering guidance and recommended countermeasures for emerging cyber risks and trends.
- NSA's role as both a source of cyber threat information and as the administrator of the U.S. Intelligence Community's CRITIC alert system (defined under the U.S. Intelligence Community Directive 190), identifies them as a key partner as well.

Appendix 7: Possible Framework for Cybersecurity Information by Type and Level

	Threat	Vulnerability	Dependency
Strategic *Long-term data and analysis that captures, assesses, and forecasts trends, directly informing an organization's year-over-year cybersecurity planning, budget allocation, and decision-making.* *It serves to establish the* ***baseline*** *of the cyber environment.*	Characterization and assessment of threat actor's objectives, constraints, and targeting preferences Trends and evolution of threat actor tactics, techniques, and procedures Assessment and forecast of behavioral or operational change based on external factors (geopolitical, economic, etc.).	Assessment of common or emerging methods of exploitation and intrusion Reports on emerging technology weaknesses Evaluation of procedural weaknesses against best practices	Assessment of trends in trade and supply-chain dependency. Assessment of market consolidation, acquisition, or other factors that shift centralization of risk Assessments or identification of cross-sector dependencies Assessment of common technology products or services shared among enterprises
Operational *Data and information from routine assessments, ad hoc reporting, and forecasts or assessments that report deviations from baseline to address cybersecurity issues in day-to-day operations.*	Updates to cyber threat actor behavior and tactics Identification and disclosure of on-going campaigns Monitoring of deep and dark web hacking forums Assessment of shifts in geopolitical factors (tension, conflict)	Risk and vulnerability assessments External audit or remote vulnerability scanning Red-teaming and penetration testing Notice of deprecation of support to product	Monitoring third-party security (External audits of critical vendors) Risk assessments for key dependencies (Industry or government reports) External dependency assessments
Tactical *Encompasses information that is intended to inform or prompt immediate action, often with the aim of discovering, preventing, or mitigating a near-term harm.*	Published or shared Indicators of compromise Victim notification of compromise News reporting	Notifications of newly-discovered vulnerabilities. Immediate patching and mitigation (vendor remote update) Notification of vulnerability (CISA scan)	Notice of planned outage (vendor or government communication) Vendor disclosure of compromise or incident

Appendix 8: Parallels and Differences Between a prospective national cybersecurity alert system and the U.S. National Weather Alert System

Similarities:

- Addresses a hazard shared by ‘many’ (weather or cyber threat)
- Establishes efficient and effective mechanisms for collection and dissemination of hazard information from party(ies) to affected parties
- General information about strategic weather patterns Is differentiated from specific tactical warning
- Has both push and pull modalities

Differences:

- Weather does not adjust to changes in its victims’ disposition or awareness; Cyber threat actors do
- Weather holds all in its path at common risk (broadcast modes appropriate); Cyber is often more selective (selective dissemination)

Appendix 9: Parallels and Differences between a prospective national cybersecurity alert system and the National Terrorism Advisory System

Similarities:

- Addresses a hazard shared by ‘many’ (e.g., terrorism by one, cyber threat by the other)
- Both systems aim to create efficient and effective mechanisms for collection and dissemination of hazard information from party(ies) to affected parties
- Warnings may be either general or specific - General information about strategic threat level is differentiated from specific, imminent, and tactical warning (the latter is preferred)
- The threat can/does react and change based on the awareness and preparation of intended victims

Differences:

- Most of the tools to prepare, mitigate threat, and defend from fist response through recovery are in the private sector (in the GWOT, the government was the principal actor for counterterrorism; Notifications were largely intended to reduce the attack surface in/of private citizens and their materiel. In cyber, a warning may be intended to stimulate a defensive action by a private sector entity whose actions then mitigate threat and/or extend protections to others).

Appendix 10: Additional Resources

Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)

https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia

CISA National Cyber Incident Scoring System (NCISS), September 30, 2020

https://www.cisa.gov/news-events/news/cisa-national-cyber-incident-scoring-system-nciss

Presidential Policy Directive – United States Cyber Incident Coordination, July 26, 2016

https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident

CISA Stakeholder-Specific Vulnerability Categorization (SSVC)

https://www.cisa.gov/stakeholder-specific-vulnerability-categorization-ssvc

U.S. Intelligence Community Critical Information (CRITIC) Program

https://www.dni.gov/files/documents/ICD/ICD%20190.pdf

Homeland Security Advisory Council, Homeland Security Advisory System Task Force Report and Recommendations, September 2009

https://www.dhs.gov/xlibrary/assets/hsac_task_force_report_09.pdf