неофіційний переклад

Система обміну інформацією прозагрози для критичної інфраструктури

Довідковий посібник дляспільноти критичної інфраструктури

Жовтень 2016 рік

Зміст

Короткий довідник для
Власників та операторів об'єктів критичної інфраструктури[1, 2]

Повідомляти про загрози та інциденти

- У надзвичайних ситуаціях телефонуйте 9-1-1, повідомляйте про підозрілу діяльність та загрози федеральним об'єктам за номером 1- 877-4FPS-411 (1-877-437-7411)
- Зверніться до місцевого правоохоронного органу
- Звітуйте через відповідний внутрішній процес звітування вашої місцевої організації
- Повідомляйте про загрози та інциденти, що не є надзвичайними, безпосередньо до найближчого відділення FBI за адресою https://www.fbi.gov/contact-us/field або до найближчого міжнародного офісу заадресою https://www.fbi.gov/contact-us/legat
  - Повідомляйте про загрози та злочини онлайн на https://www.fbi.gov/report-threats-and-crime
  - Повідомляйте про підозрілу діяльність, пов'язану з хімічними, біологічними або радіологічними матеріалами, за телефоном (безкоштовно) 1-855-TELL-FBI (1- 855-835-5324)
  - Повідомляйте про шахрайство в Інтернеті або підозрілу електронну пошту, подавши скаргу до Центру розгляду скарг на злочини в Інтернеті за адресою http://www.ic3.gov/complaint/default.aspx або скориставшись онлайн-формою "Поради та повідомлення громадськості" за адресою https://tips.fbi.gov/.
  - Надайте інформацію про окремі вагомі справи, зателефонувавши до Контактногоцентру з вагомих справ за номером 1-800-CALL-FBI (1-800-225-5324)

Повідомити про підозрілу активність

Щоб повідомити про підозрілу діяльність, зверніться до місцевого правоохоронного органу. Опишіть, що саме виспостерігали, зокрема:

- **Кого** або **що** ви бачили, включаючи підозріле ім'я користувача та скріншот, якщовін онлайн
- **Коли** ви побачили це
- **Де** це сталося, включаючи веб-посилання, якщо онлайн
- **Чому** це підозріло
- **Як** стався інцидент (тобто, як підозрюваний увійшов до будівлі, як ви виявили, що щось не так)

У разі надзвичайної ситуації телефонуйте 9-1-1.

ЧОМУ ПОВІДОМЛЯТИ ПРО ІНЦИДЕНТИ?

Для розкриття кіберзлочинів та інцидентів потрібні дані. Коли про інциденти повідомляють з найкращими доступними даними, правоохоронці та фахівці з безпеки мають більше шансів розкрити злочини і запобігти майбутнім наслідкам не лише від причетних до них суб'єктів, але й від тих, хто використовує ту ж інфраструктуру

---

[1] Ця Рамкова програма зосереджена на обміні інформацією на основі структур *Національного плану захисту інфраструктури (NIPP) 2013 року*; однак деякі сектори, такі як хімічний, ядерний, медичний та сектор охорони здоров'я, мають регуляторні вимоги щодо повідомлення про інциденти до своєї регуляторної програми. Ця Рамкова програма не розглядає ці регуляторні вимоги.

[2] Як описано в Розділі 1.2 "Мета та сфера застосування", сфера застосування цієї Рамкової програми обмежуєтьсяантропогенними загрозами.

Повідомляйте про підозри або відомі кіберінциденти

- Зверніться до Національного центру інтеграції кібербезпеки та зв'язку (NCCIC) за адресою: https://www.dhs.gov/about-national-cybersecurity-communications- integration-center, nccic@hq.dhs.gov або 1-888-282-0870
- Для отримання додаткової інформації див. опис структури NCCIC на сторінці 31
- Зверніться до найближчого відділення FBI: http://www.fbi.gov/contact-us/field
- Див. двосторінкове резюме щодо звітності про кіберінциденти, зокрема, коли, про що і як повідомляти про кіберінциденти федеральному уряду (призначене для правоохоронних органів, але також актуальне для власників та операторів об'єктів критичної інфраструктури): https://dhs.gov/sites/default/files/publications/Law Enforcement Cyber Incident Reporting.pdf

Повідомляти про інциденти фізичної інфраструктури

- Напишіть до Національного інфраструктурного координаційного центру (NICC) на електронну адресу NICC@hq.dhs.gov або зателефонуйте (202) 282-9201
- Зверніться до Організації з обміну та аналізу інформації (ISAO) або Центруобміну та аналізу інформації (ISAC) та/або до галузевого агентства (SSA) у вашому секторі

Станьте партнером кампанії "Якщо ти щось бачиш,скажи щось™"

- Для отримання додаткової інформації відвідайте https://www.dhs.gov/see-something-say-something/become-partner

Отримуйте інформацію про загрози, що стосуються вашого сектору

Існує безліч способів отримання інформації про загрози. Власники та оператори об'єктів критичної інфраструктури, ймовірно, захочуть зв'язатися з більш ніж однією з перелічених нижче організацій, щоб налагодити постійний обмін інформацією. Вибір організації, яка найкраще підходить для вашої організації, може залежати від ваших потреб, можливостей та інтересів. Більш детальну інформацію про ці та інші організації, що обмінюються інформацією про загрози, див. в описі організацій у Розділі 3, починаючи зі стор. 21.

- Зверніться до місцевого правоохоронного органу (для отримання додаткової інформації див. опис місцевих та державних оперативних центрів правоохоронних органів на сторінці 30).
- Зверніться до найближчого відділення FBI https://www.fbi.gov/contact-us/field (див. опис відділень FBI на сторінці 23 для отримання додаткової інформації)
- Приєднуйтесь до Інформаційної мережі національної безпеки - критична інфраструктура (HSIN-CI) https://www.dhs.gov/hsin-ci (див. опис структури NICC на сторінці 33 для отримання додаткової інформації)
- Приєднуйтесь до Регіональної координаційної ради консорціуму (RC3) увашому регіоні -Заявка на членство та посилання на членів Ради: http://RC3US.org
- Приєднайтесь до програми InfraGard-Membership та отримайте доступ до захищеного веб-порталу InfraGard: http://www.infragard.org. Приєднуйтесь до ISAO

вашого сектору або регіону, або до ISAC вашого сектору

- Для отримання додаткової інформації, включаючи повний перелік веб-сайтів ISAC, див. опис організації ISAO на стор. 27 та опис організації ISAC на стор. 26, або відвідайте веб-сайт Національної ради ISAC: http://www.isaccouncil.org.

- Зверніться до найближчого Об'єднаного центру штатів і головних міських районів і попросіть про брифінг або встановіть відносини для обміну інформацією
  - Знайдіть найближчий центр синтезу: http://www.dhs.gov/contact-fusion-centers
  - Зв'яжіться з офіцером зв'язку Об'єднаного центру для роботи з приватним сектором
  - Для отримання додаткової інформації див. опис організації "Об'єднаний центр" на стор. 25
  - Зверніться до свого SSA або Секторальної координаційної ради (SCC). Опис SCC , перелік Секторальних координаційних рад та їхніх веб-сайтів див. на стор. 38.
  - Статути та інформацію про сектори для Координаційних рад секторів та Урядових координаційних рад можна знайти на сайті https://www.dhs.gov/critical-infrastructure- partnership-advisory-council
  - На сторінці 40 ви знайдете опис SSA, а на сторінці 41 - список SSA та їхню контактну інформацію.

Доступ до тренінгів та навчань, пов'язаних із запобіганням загрозам тазахистом

- На сайті https://www.dhs.gov/critical-infrastructure-training ви знайдете широкий спектр безкоштовних тренінгів, спрямованих на покращення знань та навичок, необхідних для впровадження заходів з безпеки та стійкості критично важливої інфраструктури, включаючи підготовку до активних дій та саморобних вибухових пристроїв.
- Безкоштовний онлайн-тренінг з повідомлення про підозрілу активність (SAR) для приватного сектору та інших партнерів у сфері безпеки в рідному місті доступний за посиланням: https://nsi.ncirc.gov/training_online.aspx.
- Зверніться до найближчого відділення FBI, яке має координаторів з питань роботи з населенням у кожному з 56 відділень. Повний перелік тренінгів та освітньої інформації див. на стор. 23
  - Для отримання додаткової інформації про роботу FBI з громадськістю відвідайте https://www.fbi.gov/about- us/partnerships_and_outreach/community_outreach та https://www.fbi.gov/about/partnerships/office-of-partner-engagement/active-shooter-incidents
- Зверніться до найближчого Об'єднаного центру (стор. 25), найближчого радника з питань захисту інфраструктури (DHS) Департаменту внутрішньої безпеки (DHS) (стор. 37), секторального ISAC (стор. 26) або секторальної координаційної ради (SCC) (стор. 38), щоб дізнатися більше про можливості.

Резюме

Ця Рамкова програма є ресурсом, який допоможе власникам та операторам об'єктів критичної інфраструктури, а також іншим партнерам з приватного сектору, федерального уряду та уряду штатів, місцевих, племінних і територіальних утворень (SLTT), які обмінюються інформацією про загрози, дізнатися, куди вони можуть звернутися і за яких обставин, щоб отримати інформацію про загрози та повідомити про них. Інформація про загрози в цій Рамковій програмі обмежується обміном інформацією, що стосується антропогенних загроз, включаючи кібернетичні та фізичні загрози для критичної інфраструктури.

Цей документ не є новою політикою, але описує різні процеси і механізми, які зараз використовуються для обміну інформацією про загрози, а також існуючий набір суб'єктів обміну інформацією про загрози, залучених до цих процесів. Він був розроблений у відповідь на потребу в більшій ясності, виявлену спільнотою критичної інфраструктури, і підтримує *Національну стратегію обміну та захисту інформації* 2012 року (NSISS)[3] а також *Національний план захисту інфраструктури (NIPP) 2013 року: Партнерство заради безпеки та стійкості критичної інфраструктури* (NIPP 2013)[4] Заклик до дій, спрямований на розвиток партнерства, однією з цілей якого є обмін практичною та актуальною інформацією в рамках спільноти, що займається питаннями критичної інфраструктури.

У Розділі 1 викладено передумови, мету, сферу застосування та цільову аудиторію Рамкової програми. У ньому також визначено керівні принципи обміну інформацією, вибрані з найбільш релевантних стратегічних і політичних документів, що стосуються цієї Рамкової програми. Розділ 2 містить огляд процесу обміну інформацією про загрози та типів суб'єктів обміну інформацією про загрози за категоріями. Розділ 3 містить односторінкові описи основних партнерів з обміну інформацією про загрози, які беруть участь у процесі обміну інформацією про загрози, описаному в попередньому розділі. Описи включають контактну інформацію, продукти і послуги, доступні для власників і операторів, а також ситуації, в яких слід звертатися до конкретного суб'єкта.

У розділі 4 наведено чотири практичні приклади, які ілюструють, як обмін інформацією про загрози відбувався в реальних ситуаціях, і дають уявлення про види обміну, що відбуваються у спільноті критичної інфраструктури. Приклади використання такі:

1. Кібер: Havex та BlackEnergy (2014)
2. Фізична: Напад на електричну підстанцію в Меткалфі (2013)
3. Міжнародна: Напад на торговий центр Westgate в Кенії (2013)
4. Національна подія спеціального характеру: Інавгурація Президента України 2013 року

Використовуючи структуру ради NIPP, ця концепція була розроблена робочою групою, до складу якої увійшли представники приватного сектору, федерального уряду та SLTT, що представляють інфраструктурну спільноту. Ця робота проводилася під спільним керівництвом Федерального бюро розслідувань (FBI) і Міністерства внутрішньої безпеки (DHS). Учасники з різних секторів критичної інфраструктури оцінили поточні загрози, поточне середовище обміну інформацією, необхідні сфери для вдосконалення і конкретнівимоги, пов'язані з обміном інформацією про загрози. Протягом усього процесу розробки запитувався і враховувався зворотній зв'язок.

[3] Білий дім, *Національна стратегія обміну та захисту інформації* (NSISS), грудень 2012 р., https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (дата звернення: 17 червня 2016 р.).Міністерство внутрішньої безпеки США, *Національний план захисту інфраструктури (NIPP) 2013: Партнерство заради безпеки та стійкості критичної інфраструктури,* https://www.dhs.gov/sites/default/files/publications/National-Infrastructure- Protection-Plan-2013-508.pdf (дата перегляду: 17 червня 2016 р.). NIPP 2013 є наступником Національного плану захисту інфраструктури 2010 року.

Вступ

Наша національна безпека залежить від здатності нації ділитися потрібною інформацією з потрібними людьми в потрібний час.[5]

- 2012 Національна стратегія обміну та захисту інформації (НСЗІ)

1.1 Передумови

Критично важлива інфраструктура країни[6] надає найважливіші послуги, на яких ґрунтується американське суспільство і які слугують основою економіки, безпеки та здоров'я нашої країни. Ми знаємо, що це електроенергія, яку ми використовуємо в наших будинках, вода, яку ми п'ємо, транспорт, який переміщує нас, магазини, в яких ми робимо покупки, і системи зв'язку, на які ми покладаємося, щоб залишатися на зв'язку з друзями і родиною. Середовище ризиків, що оточує критичну інфраструктуру, є складним і невизначеним, оскільки загрози, вразливості та наслідки продовжують розвиватися.

Наприклад, критична інфраструктура, яка вже давно піддається ризикам, пов'язаним з фізичними загрозами та стихійними лихами, зараз все частіше піддається кібер-ризикам. Зростаюча взаємозалежність між системами критичної інфраструктури збільшує тип і масштаби потенційних наслідків, пов'язаних з компрометацією базових систем або мереж.[7] Враховуючи важливість критичної інфраструктури для функціонування нашої держави, життєво важливо забезпечити безпеку і стійкість цих систем і активів перед обличчям нових і все більш складних небезпек і загроз.

Як описано в *Національному плані захисту інфраструктури (NIPP) 2013: Партнерство заради безпеки та стійкості критичної інфраструктури* (NIPP 2013) (наступник *Національного плану захисту інфраструктури 2010)*,[8] виданий на виконання *Президентської політичної директиви 21 (PPD-21) "Безпека та стійкість критичної інфраструктури"*,[9] значна частина об'єктів критичної інфраструктури в Сполучених Штатах перебуває у власності та/або під управлінням приватного сектору.[10] Таким чином,

щоб забезпечити безпеку та стійкість критичної інфраструктури країни, федеральний уряд повинен розвивати міцне партнерство з власниками та операторами критичної інфраструктури. Зміцнення та підтримка безпечної та стійкої критичної інфраструктури залежить не лише від адекватних інвестицій та фізичного і віртуального захисту наших критично важливих активів і систем. Скоординовані зусилля і партнерство між приватним і державним секторами також залежать від ефективного і результативного обміну інформацією між власниками і операторами об'єктів критичної інфраструктури, Федеральним Урядом та спільнотою критичної інфраструктури[11] в цілому.

---

[5] Білий дім, *Національна стратегія обміну та захисту інформації* (NSISS), грудень 2012 р., https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (дата звернення: 17 червня 2016 р.), 1.

[6] За визначенням Патріотичного акту США (H.R. 3162, 107th Конгрес, 2001), критична інфраструктура - це "системи та активи, фізичні чи віртуальні, настільки життєво важливі для Сполучених Штатів, що їхня непрацездатність або руйнування матимуть виснажливий вплив на безпеку, національну економічну безпеку, національне здоров'я чи безпеку населення або будь-яку комбінацію цих питань".

[7] Міністерство внутрішньої безпеки США, *Національний план захисту інфраструктури (NIPP) 2013: Партнерство заради безпеки та стійкості критичної інфраструктури*, https://www.dhs.gov/sites/default/files/publications/National-Infrastructure- Protection-Plan-2013-508.pdf (дата звернення: 17 червня 2016 р.), 8[8] Більш детальну інформацію про NIPP 2013 можна знайти на сайті https://www.dhs.gov/national-infrastructure- protection-plan (дата звернення: 17 червня 2016 року).

[9] PPD-21 можна знайти за посиланням: https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy- directive-critical-infrastructure-security-and-resil (дата перегляду: 17 червня 2016 року).[10] Федеральні, регіональні та місцеві органи влади також володіють та експлуатують критично важливу інфраструктуру.

Визнаючи це, одна з п'яти цілей, сформульованих у NIPP 2013 року, зосереджена на обміні інформацією про критичну інфраструктуру:

> Діліться практичною та актуальною інформацією з усією спільнотою критично важливої інфраструктури, щоб підвищити обізнаність та уможливити прийняття рішень з урахуванням ризиків.[12]

Обмін інформацією про критичну інфраструктуру краще готує всі зацікавлені сторони до оцінки вразливостей критичної інфраструктури, усунення цих вразливостей, розуміння потенційних наслідків інцидентів, а також до запобігання, захисту, пом'якшення наслідків, реагування та відновлення після загроз і атак. Зусилля, спрямовані на покращення обміну інформацією між федеральним урядом та органами влади штатів і місцевого самоврядування, приватним сектором і, зокрема, спільнотою фахівців з питань критичної інфраструктури, продовжують розвиватися з урахуванням нових загроз, вразливостей і технологій, поважаючи при цьому право на приватність, громадянські свободи і необхідність розумних інформаційних гарантій.

1.2 Мета та сфера застосування

Мета цієї Рамкової концепції - описати поточні процеси, що використовуються для полегшення обміну інформацією про загрози між усіма суб'єктами, залученими до забезпечення безпеки та стійкості критичної інфраструктури, а також надати огляд ключових суб'єктів обміну інформацією про загрози, які сприяють цьому процесу. Мета - допомогти власникам і операторам об'єктів критичної інфраструктури та іншим суб'єктам краще зрозуміти, де і як вони можуть брати участь в отриманні інформації про загрози таобмінюватися нею з центрами обміну інформацією.

Після терактів 11 вересня 2001 року уряд США працював над удосконаленням стандартизованого обміну інформацією між різними галузями та спільнотами. Хоча ця Рамкова програма зосереджена на спільноті критичної інфраструктури, вона визнає, що процеси обміну інформацією є міждисциплінарними за своєю природою. Ця Рамкова концепція не пропонує нової політики, а спирається на існуючі повноваження, стратегії, політику, плани та практики, які визначають ролі та обов'язки федеральних департаментів та агентств, а також інших суб'єктів спільноти критичної інфраструктури, які обмінюються інформацією про загрози.[13]

Сфера застосування цієї Рамкової програми обмежується обміном інформацією про загрози, що стосуються антропогенних загроз, включаючи кібер- та фізичні загрози для критичної інфраструктури.[14] У деяких секторах, таких як хімічна, ядерна промисловість, охорона здоров'я та громадське здоров'я, існують нормативні вимоги до власників та операторів повідомляти про інциденти своїм регуляторним органам. Ця Рамкова програма не розглядає ці вимоги.

Метою цієї Рамкової програми є посилення ефективного та результативного обміну точною, дієвою, своєчасною та релевантною інформацією про загрози між федеральними органами виконавчої влади та органами виконавчої влади суб'єктів федерації.

[11] Згідно з визначенням, наведеним у NIPP 2013, спільнота критичної інфраструктури включає власників та операторів критичної інфраструктури, як державних, так і приватних, торгові асоціації, федеральні департаменти та відомства, регіональні організації, уряди країн малого та середнього бізнесу та інші організації приватного та некомерційного секторів, які відіграють важливу роль у забезпеченні та посиленні стійкості критичної інфраструктури країни та/або просуванні ідей щодо цього, а також, в деяких випадках, іноземних урядових партнерів.

[12] НІПП 2013, 5.

[13] Зважаючи на основну аудиторію цього документа (власники та оператори об'єктів критичної інфраструктури (див. розділ 1.3)), визначення всіх таких органів та політик виходить за рамки цього документа. Така інформація міститься в *Національній стратегії обміну інформацією* 2007 року та інших програмних документах, які можна знайти на сайті www.ise.gov.

[14] Ця Рамкова програма не є узагальненням НСРСІ 2012 року, НІПП 2013 року, або різних рамок місій відповідно до ППД-8, або середовища обміну інформацією. Існує безліч практик, процесів і програм обміну інформацією в уряді. Ця Рамкова концепція призначена для того, щоб зосередитися виключно на загрозах критичній інфраструктурі. Аналогічно, інформація та інформаційні потоки, пов'язані з реагуванням, розглядаються в документах, пов'язаних з PPD-8 та Рамковою програмою реагування.

Такий обмін інформацією підвищує обізнаність про ситуацію, уможливлює ефективне прийняття рішень з урахуванням ризиків,[15] а отже, підвищує безпеку і стійкість критичної інфраструктури США.

1.3 Аудиторія

Основною аудиторією цієї Рамкової програми є спільнота, що займається питаннями критичної інфраструктури, з акцентом на власників та операторів критичної інфраструктури, включаючи об'єкти критичної інфраструктури, що перебувають у приватній та державній власності, а також відповідні організації приватного сектору, що займаються обміном інформацією, включаючи Центри обміну та аналізу інформації (ISACs) та Організації з обміну та аналізу інформації (ISAOs).

Ця Рамкова концепція призначена не лише для основної аудиторії, але й для широкого кола фахівців у сфері критичної інфраструктури, включаючи галузеві відомства (SSA);[16] Федеральні центри, такі як Національний інфраструктурний координаційний центр (NICC) та Національний центр інтеграції кібербезпеки та зв'язку (NCCIC);[17] уряди штатів, місцеві, племінні та територіальні уряди (SLTT); та інші організації, залучені до процесу обміну інформацією про загрози. Наприклад, оскільки фізична критична інфраструктура розташована в межах і, відповідно, підпадає під юрисдикцію певних держав, урядові органи цих держав мають важливі обов'язки щодо запобігання, захисту, пом'якшення наслідків, реагування і відновлення після різноманітних загроз і небезпек, які можуть вплинути на критичну інфраструктуру. Урядові установи SLTT, такі як державні та великі міські об'єднані центри (об'єднані центр), також є важливим географічним контекстом,[18] також забезпечують важливий географічний контекст, аналітичні можливості і предметну експертизу для своїх юрисдикцій, посилюючи потік інформації про загрози між федеральним урядом і приватним сектором.

1.4 Керівні принципи

Ця Рамкова програма відповідає керівним принципам, викладеним у *Національній стратегії обміну та захисту інформації* (NSISS) 2012 року,[19] основним принципам NIPP 2013 року та настановам щодо середовища обміну інформацією.[20] Визнаючи, що 16 критично важливих

---

[15] NIPP 2013.

[16] PPD-21 визначає "галузеве агентство" (SSA) як федеральний департамент або агентство, призначене відповідно до цієї директиви відповідальним за надання інституційних знань і спеціалізованої експертизи, а також за керівництво, сприяння або підтримку програм безпеки і стійкості та пов'язаних з ними заходів у визначеному ним секторі критичноїінфраструктури в умовах усіх видів небезпек.

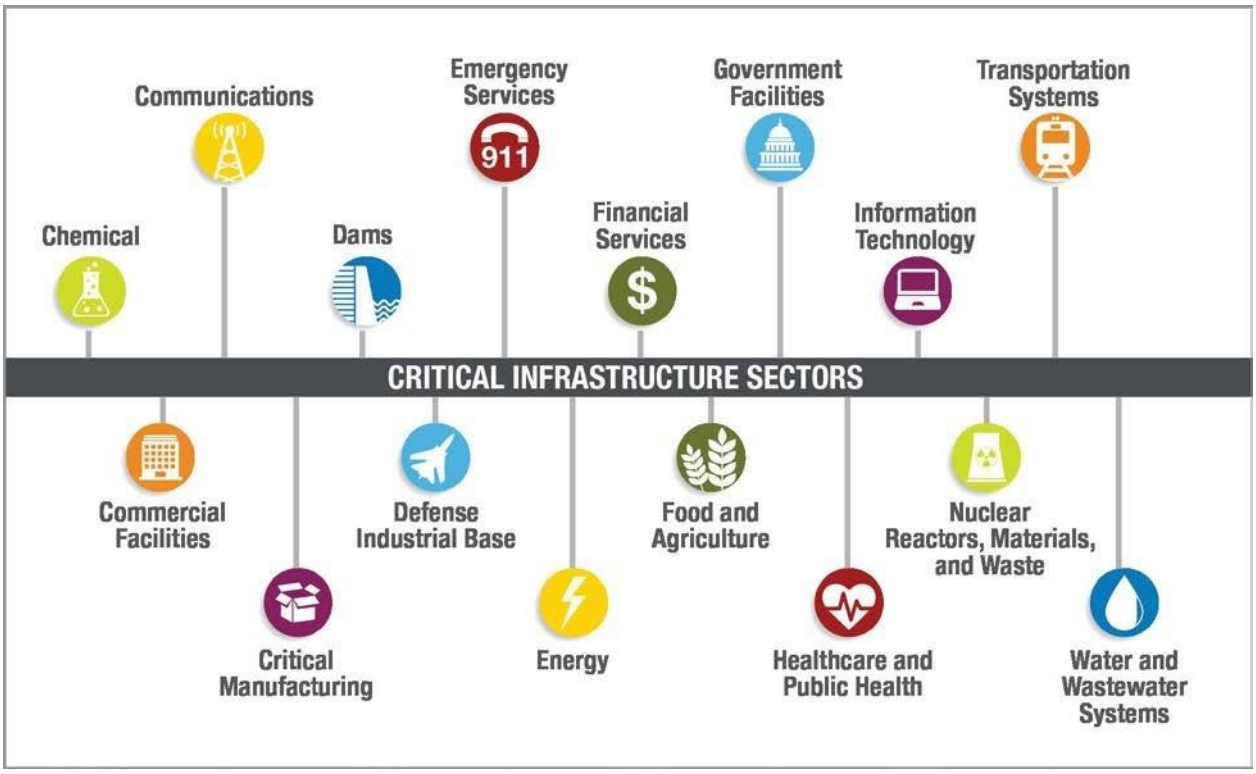
[17] Національні центри критичної інфраструктури, як описано в ППР-21.

[18] Для отримання додаткової інформації про об'єднані центри дивіться опис організації в Розділі 3 на сторінці 25.

[19] NSISS 2012 року - це план Президента щодо того, як федеральний уряд буде відповідально ділитися і захищати інформацію, яка зміцнює національну безпеку і захищає безпеку американського народу. З ним можна ознайомитися на сайті https://www.whitehouse.gov/sites/default/files/docs/2012sharingstrategy_1.pdf (дата перегляду: 17 червня 2016 року).

[20] Середовище обміну інформацією (ISE) - це люди (федеральний уряд, уряд штату, регіональні, місцеві органи влади та органи приватного сектору), проекти, системи та агенції, які забезпечують відповідальний обмін інформацією в рамках підприємства національної безпеки. ISE було створено Законом про реформування розвідки і запобігання тероризму 2004 року - прямим результатом рекомендацій Комісії з розслідування подій 11 вересня. Адміністративне управління ISE здійснює керівник програми з питань середовища обміну інформацією (PM-ISE), який має загальноурядові повноваження щодо планування, нагляду і управління ISE. Призначений Президентом, PM-ISE також є співголовою Міжвідомчого комітету Білого дому з питань обміну інформацією та доступу до неї (ISA-IPC). Роль PM-ISE полягає в координації та сприянні розвитку мережевого середовища обміну інформацією про тероризм і внутрішню безпеку, зосереджуючись на стандартах і архітектурі, безпеці і доступі, пов'язаному з ними захисті конфіденційності та передовому досвіді. PM-ISE виступає агентом змін і центром інновацій та відкриттів, надаючи ідеї, інструменти та ресурси партнерам місії, які потім застосовують їх у своїх відомствах або громадах.

секторів інфраструктури[21] різноманітні за своїм складом, загрозами, вразливостями, активами, системами та регуляторними режимами, ця Рамкова програма підтримує широкий спектр галузевих перспектив, операцій та рівнів прийняття рішень.



Малюнок 1: 16 секторів критичної інфраструктури

Під час розробки цієї Рамкової концепції були визначені наступні принципи обміну інформацією про загрози, які були розроблені на основі NSISS. Ці принципи слід враховувати при обміні інформацією про загрози.

1. Для ефективного прийняття рішень інформація, якою обмінюються, має бути точною, доречною, своєчасною і такою, що спонукає до дій.

2. Щоб бути максимально ефективним, обмін інформацією повинен бути багатовекторним. Інформацію про загрози, коли це можливо, слід передавати партнерам по критичній інфраструктурі на відповідному рівні секретності. Надання доступу до конкретної та дієвої несекретної інформації про загрози, такої як "лінії розриву", брифінги[22] JIBs, брифінги тощо, дасть змогу якомога більшій кількості зацікавлених сторін обмінюватися нею у своїх організаціях та вживати заходів для пом'якшення загроз.

3. Ризики, пов'язані з обміном інформацією та її захистом, зменшуються завдяки прийняттю надійних політик і стандартів. Побудова довіри в обміні та

[21] ППР-21 визначає 16 секторів критичної інфраструктури.

[22] Інформація "лінії розриву" - це розвідувальна інформація, яка пройшла санітарну обробку (шляхом видалення джерел і методів), щоб її можна було поширювати з нижчим ступенем секретності. Джерело: Посібник з розвідки для тих, хто здійснює перше реагування, Об'єднана група з оцінки контртерористичної діяльності (JCAT),

https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf (дата перегляду: 17 червня 2016 р.).

захисті вимагає здатності управляти ризиками. Ризик для національної безпеки зростає, коли підхід до обміну інформацією є непослідовним, фрагментарним або здійснюється з точки зору одного відомства. Ризик зменшується завдяки надійній політиці та стандартам, підвищенню обізнаності та всебічному навчанню, ефективному управлінню та посиленню підзвітності.[23]

Крім того, при розробці цієї Рамкової концепції було використано проект *Посібника з обміну інформацією про кіберзагрози* Національного інституту стандартів і технологій (NIST Special Publication 800-150).[24]

1.5 Методологія розвитку

Використовуючи структуру ради NIPP, ця концепція була розроблена робочою групою, до складу якої увійшли представники приватного сектору, федерального уряду та SLTT, а також представники інфраструктурного співтовариства. Ця робота проводилася під спільним керівництвом Федерального бюро розслідувань (FBI) і Міністерства внутрішньої безпеки (DHS). Учасники різних секторів критичної інфраструктури оцінили поточні загрози, поточне середовище обміну інформацією, необхідні сфери для вдосконалення і конкретні вимоги, пов'язані з обміном інформацією про загрози. Протягом усього процесу розробки запитувався зворотній зв'язок, який був врахований.

[23] NSISS, 7.

[24] Другий проект Спеціальної публікації NIST 800-150 був випущений у квітні 2016 року і на момент написання цієї статті не був опублікований в остаточному вигляді. З ним можна ознайомитися на сайті http://csrc.nist.gov/publications/PubsDrafts.html#SP-800-150 (дата перегляду 17 червня 2016 року).

Огляд обміну інформацією про загрози безпеці та стійкості критичної інфраструктури

У цій Рамковій програмі сформульовано гнучкий, адаптивний і мережевий підхід до обміну інформацією про загрози, який спирається насамперед, але не виключно, на визначені центри обміну інформацією[25] які виконують певні функції та обов'язки в рамках місії із забезпечення безпеки та стійкості критичної інфраструктури та використовують стандарти, базові можливості та/або стандартні операційні процедури (SOPs) для забезпечення інформаційних потоків до та від усіх партнерів з критичної інфраструктури. Ця Рамкова програма також відображає потребу в гнучкості та масштабованості і враховує важливість і корисність неформальних мереж,[26] забезпечуючи, за необхідності, спеціальний зв'язок "точка-точка". Гнучка структура дозволяє ефективно реагувати на нові загрози, дотримуючись при цьому різних гарантій і обмежень на обмін інформацією. Масштабована структура дозволяє розширювати і скорочувати обсяг обміну інформацією залежно від конкретної загрози.

Як зазначено в Розділі 1, ця Концептуальна основа не пропонує нової політики. Цей підхід ґрунтується на принципах, визначених у стратегіях і планах національної безпеки Уряду США, які визнають, що розмір країни, вільний ринок і федеративний устрій у поєднанні з мінливим і багатогранним характером загроз, що стоять перед США, вимагають від США використання загальнодержавного і загальносуспільного підходу до запобігання і пом'якшення загроз. Федеральний уряд співпрацює з урядами малих і середніх міст, приватним сектором і громадянами та покладається на них у запобіганні, захисті, реагуванні, пом'якшенні та відновленні після різноманітних загроз. Цей підхід значною мірою спирається на ефективний обмін інформацією з усіма партнерами.

Ця Рамкова концепція документує поточне середовище, що розвивається, і визначає ключові центри та інших учасників мережі, через які проходять інформаційні потоки. У ній акцентується увага на тих суб'єктах, які мають прямий зв'язок з власниками та операторами об'єктів критичної інфраструктури (тобто на тих суб'єктах, з якими власники та оператори можуть обмінюватися інформацією або отримувати її). Ця Рамкова концепція також визнає, що в правоохоронних органах, органах національної безпеки та розвідки існує багато організацій, які виробляють інформацію, що може бути цінною для власників та операторів об'єктів критичної інфраструктури, навіть якщо ці організації не мають прямої взаємодії з власниками та операторами об'єктів критичної інфраструктури.

Важливою частиною цієї Рамкової програми та описаного в ній процесу обміну інформацією є ідея про те, що центри обміну інформацією мають найкращі можливості для оцінки інформації в контексті їхнього досвіду та спільноти, якій вони служать.
Прикладами центрів обміну інформацією у федеральному уряді є Центр скринінгу тероризму FBI (TSC), Національний контртерористичний центр (NCTC), Національний інфраструктурний координаційний центр (NICC) та Національний центр інтеграції кібербезпеки та зв'язку (NCCIC).[27]

[25] Центри обміну інформацією (хаби) більш детально описані в розділі 2.1. Загалом, хаби - це організації, які агрегують, інтегрують, перевіряють, оцінюють та аналізують інформацію, а також створюють та обмінюються продуктами. У цій Рамковій програмі основна увага приділяється хабам, які створюють інформацію про загрози, що має відношення до місії із забезпечення безпеки та стійкості критичної інфраструктури.

[26] Офіційного визначення неформальних мереж обміну інформацією не існує. Як правило, вони базуються на особистих контактах і мають ситуативний характер. Іноді люди використовують неформальні мережі для того, щоб обійти уявні або реальні бар'єри чи виклики, пов'язані з процесом або організацією. Використання цього терміну в цій Рамковій програмі означає визнання того, що санкціонований обмін інформацією відбувається поза межами центрів обміну інформацією та процесу, описаного в Розділі 2.1, і що такий обмін сприймається як здорова частина екосистеми обміну інформацією про загрози за умови, що такий обмін здійснюється у спосіб, який відповідає всім вимогам щодо захисту інформації та захищає приватність і громадянські свободи.

Хоча кожна з цих організацій має окремі місії та ролі, всі вони є частиною процесу обміну інформацією. Наступні приклади нефедеральних центрів обміну інформацією також демонструють їхню важливість в екосистемі обміну інформацією:

- **Об'єднані центри:**[28] Національна стратегія обміну інформацією (NSIS) 2007 року визнала і кодифікувала ролі та обов'язки державних і великих міських об'єднанихцентрів в середовищі обміну інформацією. Зокрема, вона закликала до створення національної інтегрованої мережі об'єднаних центрів і визначила об'єднані центри як "основні, але не виключні пункти в державному і місцевому середовищі для отримання та обміну інформацією про тероризм, національну безпеку і правоохороннуінформацію, пов'язану з тероризмом".[29]

  Центри належать і управляються державними та місцевими органами влади. Деякі центри були створені ще до терактів 11 вересня 2001 року, але після цього концепція набрала обертів, і до 2005 року існуючі центри спільно розробили керівні принципи роботи центрів синтезу. Пізніше вони встановили базові можливості для об'єднаних центрів. Федеральний уряд підтримує об'єднані центри за допомогою різних ресурсів, включаючи доступ до засекречених і незасекречених систем, персональне і грантове фінансування.

- **Центри обміну та аналізу інформації (ISAC):**[30] ISAC були створені та управляються консорціумами власників та операторів критичної інфраструктури з метою забезпечення всебічного аналізу сектору критичної інфраструктури в межах сектору, інших секторів та з урядом. Вони здебільшого складаються з суб'єктів приватного сектору. Хоча федеральний уряд докладає зусиль по встановленню відносин з ISAC.

КІБЕР
ОБМІН ІНФОРМАЦІЄЮ

Як дисципліна, кібербезпека швидко розвивається, і створюються нові урядові та приватні організації, які займаються всіма її аспектами, що змінюються. Відносно молодий характер галузі відображає середовище, в якому необхідно часто оновлювати закони, нормативні акти, політику і керівництво, що згодом призводить до змін у процедурах і протоколах обміну інформацією про кіберзагрози. Процес обміну інформацією на високому рівні, описаний у цій Рамковій програмі, був розроблений таким чином, щоб охопити основні дії, які відбуваються незалежно від того, чи є загроза кібернетичною або фізичною. Незважаючи на те, що в найближчому майбутньому, ймовірно, відбудуться зміни в організаціях, правилах і протоколах обміну інформацією про кіберзагрози, робоча група вважає, що загальні принципи і процеси, описані в Рамковій концепції, залишаться актуальними на найближчі роки. Читачеві рекомендується відвідати ресурси, наведені в описі суб'єктів (Розділ 3), щоб ознайомитися більш детально з механізмами та процесами обміну кіберінформацією.

[27] Більш детальну класифікацію центрів обміну інформацією наведено в розділі 2.2. Опис цих та інших суб'єктів наведено в Розділі 3.

[28] Цей опис призначений для того, щоб показати, як ф'южн-центри є прикладом центру обміну інформацією. Для отримання додаткової інформації про ф'южн-центри див. більш детальний опис у Розділі 3 на стор. 25.

[29] СЗПБ 2012 року прямо підтверджує СЗПБ 2007 року.

[30] Цей опис має на меті показати, як ISAC є прикладом центру обміну інформацією. Для отримання додаткової інформації про ISAC дивіться більш детальний опис на сторінці 26.

- **Організації з обміну та аналізу інформації (ISAO):**[31] Федеральний уряд заохочує розробку добровільних стандартів і керівних принципів для створення і функціонування ISAO, які обмінюються інформацією в регіоні, секторі, підсекторі або у відповідь на конкретну нову кіберзагрозу. Організація стандартів ISAO (ISAO-SO), очолювана Техаським університетом в Сан-Антоніо, була створена 1 жовтня 2015 року і працює зі спільнотою критичної інфраструктури над визначенням загального набору добровільних стандартів для створення і функціонування ISAO відповідно до вимог Виконавчого наказу 13691 "*Сприяння обміну інформацією з кібербезпеки в приватному секторі*".[32]

Підтримка федеральним урядом центрів обміну інформацією, які дотримуються єдиних стандартів і можливостей, забезпечує ефективний і результативний обмін інформацією, водночас забезпечуючи незалежність між організаціями та різноманітність місій.

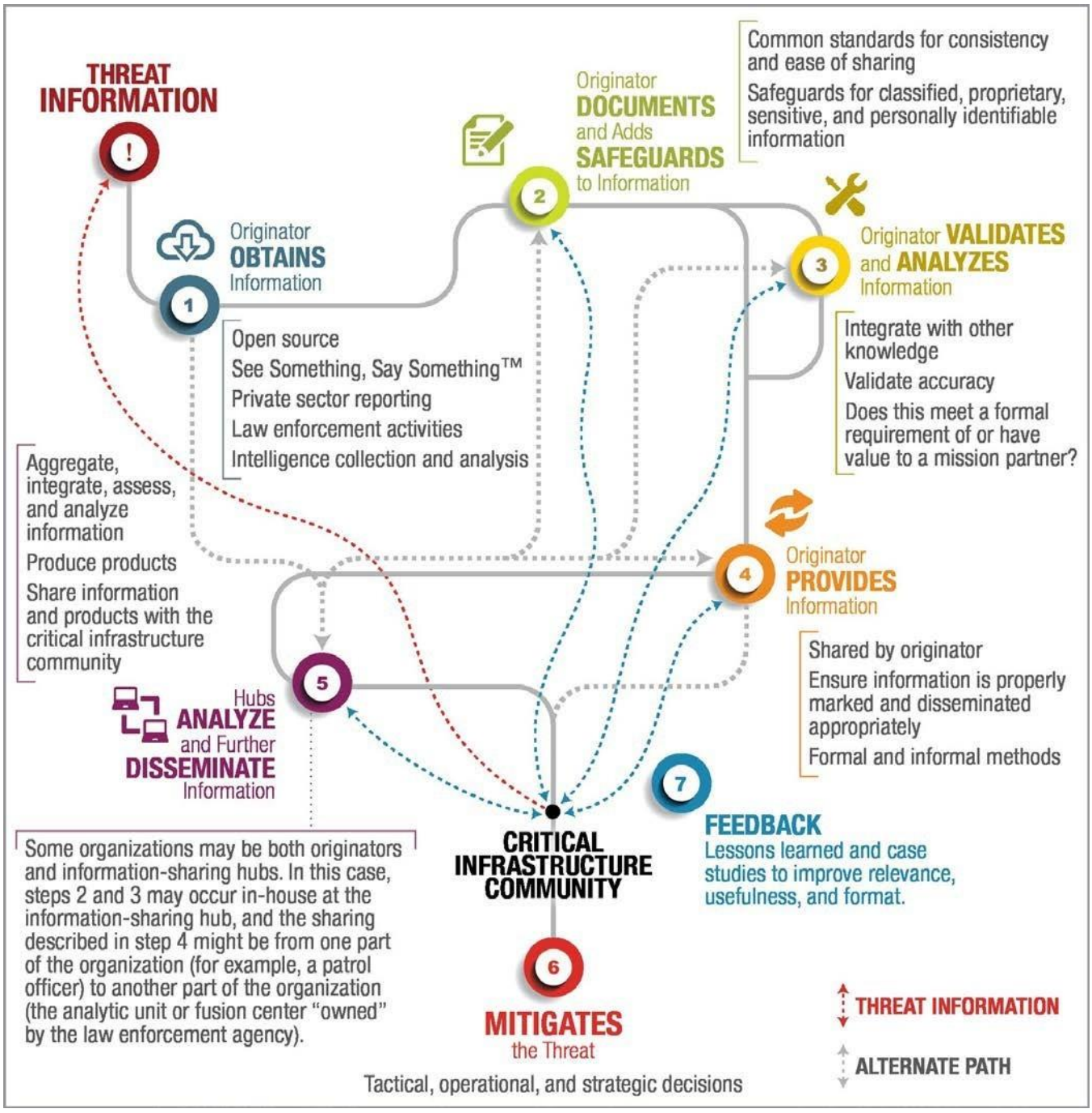
2.1 Процес обміну інформацією про загрози

У цьому розділі подано огляд процесу обміну інформацією про загрози критичній інфраструктурі та типів організацій, які беруть участь у процесі обміну інформацією про загрози критичній інфраструктурі.

Після отримання інформація рухається між державними установами та приватним сектором через багатовекторну, гнучку, децентралізовану "мережу", що характеризується як формальними, так і неформальними каналами, які описані в описах установ та різноманітних тематичних дослідженнях, наведених у розділах 3 і 4 відповідно. Однак, незважаючи на своє розмаїття, мережеві інформаційні потоки можна узагальнити у вигляді наведених нижче кроків. Порядок виконання певних кроків часто диктується внутрішніми правилами, вимогами та процедурами організації. Цей огляд процесу не означає, що організації повинні змінювати свої процедури, а окремі особи не повинні ігнорувати свої внутрішні вимоги.

[31] Цей опис має на меті показати, як ISAO є прикладом центру обміну інформацією. Для отримання додаткової інформації про ISAO дивіться більш детальний опис на сторінці 27.

[32] З Указом 13691 можна ознайомитися за посиланням: https://www.whitehouse.gov/the-press-office/2015/02/13/executive- order-promoting- private-sector-cybersecurity-information-shari (дата перегляду: 20 червня 2016 року).



Малюнок 2: Процес обміну інформацією про загрози

Цей графік не повністю відображає багатовекторну, децентралізовану мережу формальних і неформальних каналів, через які державні органи та приватний сектор обмінюються інформацією. Він призначений лише для того, щоб показати основні етапи інформаційного потоку. Залежно від розміру організації-джерела інформації, певні етапи можуть відбуватися неформально і одночасно. Деталі кожного кроку описані в описі нижче.

Крок 1: Ініціатор отримує інформацію[33]

Інформацію отримують з різних джерел (відкритих, конфіденційних, правоохоронних, розвідувальних, державних і приватних) і методів (розслідування, оцінки та збір розвідувальних даних). Наприклад, співробітники служби громадської безпеки або охорона приватної компанії спостерігають тенденцію до вразливості безпеки на об'єкті або в IT-мережах; місцеві, державні або федеральні правоохоронні органи отримують інформацію в результаті правоохоронної діяльності (наприклад, розслідувань, рутинного правозастосування тощо); громадянин помічає підозрілу активність; або Розвідувальне співтовариство (IC) федерального уряду[34] виявляє достовірну загрозу.

Крок 2: Ініціатор документує та додає засоби захисту до інформації

Найкращою практикою є розробка та оприлюднення організаціями процесів звітування про загрози та інциденти, зокрема щодо того, як і коли інформацію слід надсилати іншим організаціям, наприклад, центрам обміну інформацією. За необхідності, організації повинні дотримуватися своїх внутрішніх процедур звітування.

Як правило, кожна організація має процеси документування інформації, отриманої законним шляхом і з визначеною метою.

- Були розроблені загальні стандарти, щоб допомогти федеральним правоохоронним органам і правоохоронним органам штатів, що займаються боротьбою з нелегальним обігом наркотиків, у послідовному документуванні інформації. Стандартизація полегшує обмін інформацією. Наприклад, процес звітування про підозрілу діяльність (SAR)[35] визначає елементи даних і загальний процес, який слід використовувати для полегшення оцінки та обміну такою інформацією в належний спосіб.

У процесі документування інформація "маркується", щоб вказати на необхідний рівень захисту та будь-які обмеження щодо санкціонованого доступу або використання.
Наприклад:

- Якщо інформація отримана IC, вона може бути позначена необхідним рівнем секретності.
- Якщо вона отримана з джерел правоохоронних органів, то може мати позначку "Конфіденційна інформація для правоохоронних органів" (LES).
- Якщо інформація містить персональні дані (PII), маркування повинно відповідати правилам і рекомендаціям організації, місцевих, державних і федеральних норм і правил. Організації часто вимагають, щоб уповноважені одержувачі пройшли відповідне навчання та погодилися дотримуватися правил перед отриманням інформації.[36]

---

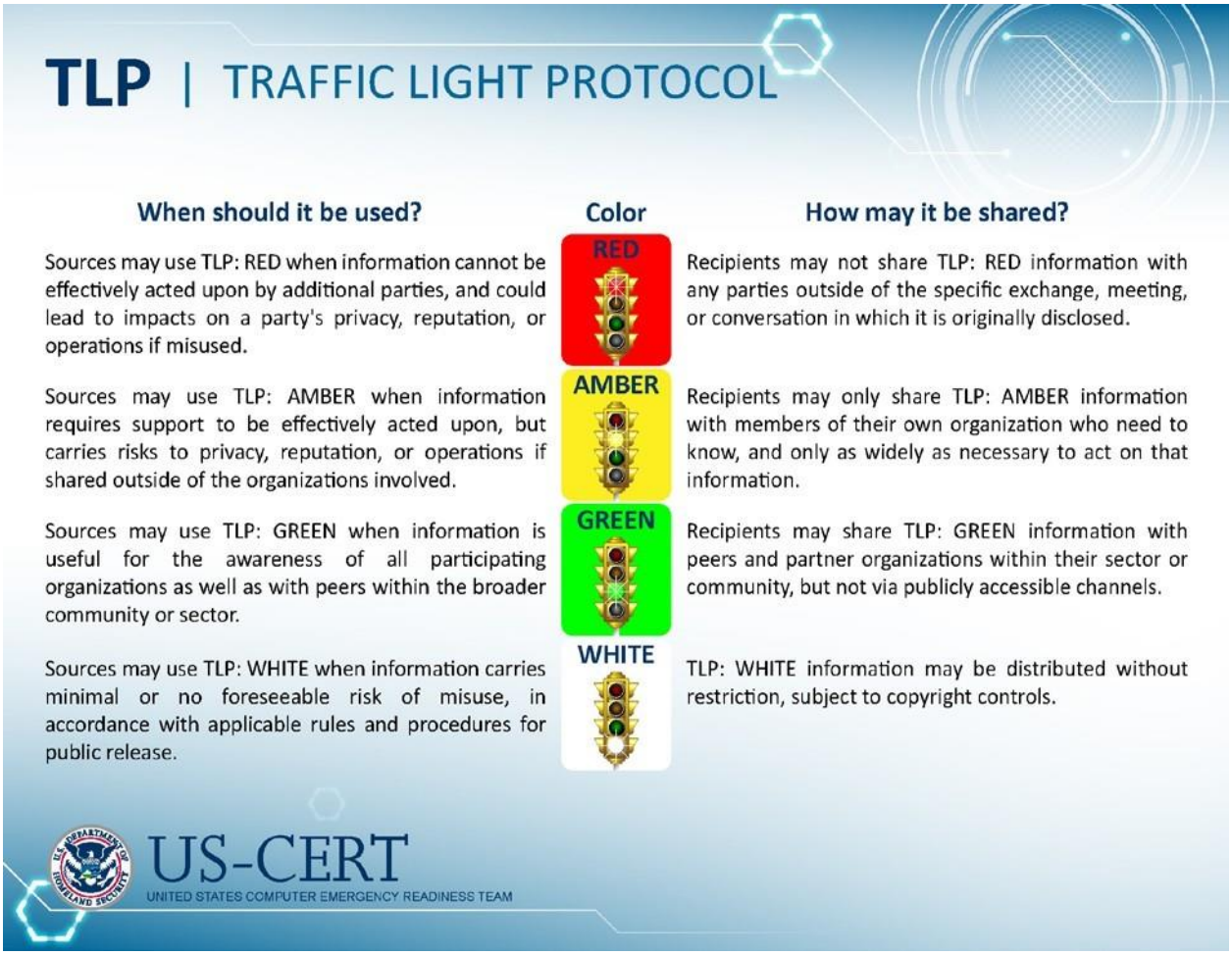
[33] На початку процесу не завжди зрозуміло, чи становить інформація загрозу, чи ні.

[34] Розвідувальне співтовариство (РС) - це група агентств і організацій виконавчої влади, які працюють окремо і спільно для здійснення розвідувальної діяльності, необхідної для ведення зовнішніх відносин і захисту національної безпеки Сполучених Штатів. Ця діяльність включає збір інформації, необхідної Президенту, Раді національної безпеки, державним секретарям і міністрам оборони та іншим посадовим особам виконавчої влади для виконання їхніх обов'язківі здійснення повноважень. Вони виробляють і поширюють розвідувальну інформацію та захищають від ворожої діяльності, спрямованої проти Сполучених Штатів. Розвідку очолює директор Національної розвідки (DNI), який очолює Офіс директора Національної розвідки (ODNI) і в обов'язки якого входить координація діяльності інших 16 компонентів розвідки, виходячи з потреб споживачів розвідувальної інформації. *Національна розвідка США: Огляд 2013*. За більш детальною інформацією звертайтеся за адресою: Partner.Engagement@dni.gov.

[35] Для отримання додаткової інформації про Загальнонаціональну ініціативу з повідомлення про підозрілу діяльність (NSI) перейдіть за посиланням https://nsi.ncirc.gov/default.aspx (дата звернення: 21 червня 2016 р.).

[36] Протоколи МК є найсуворішими, вимагаючи від одержувачів допусків (що саме по собі вимагає тривалих кроків, пов'язаних з отриманням і підтриманням допуску), підписання юридично зобов'язуючих угод про захист інформації та проходження щорічного навчання з питань поводження з секретною інформацією.

- Багато ISAC та інших організацій використовують протокол світлофора (TLP),[37] [38] набір позначень, які використовуються для того, щоб забезпечити передачу конфіденційної інформації правильній аудиторії. Він використовує чотири кольори для позначення різних ступенів чутливості та відповідних міркувань щодо обміну інформацією, які повинні застосовуватися одержувачами.



Малюнок 3: Протокол світлофора

Крок 3: Ініціатор перевіряє та аналізує інформацію

Автори, наскільки це можливо, інтегрують інформацію з іншими знаннями та перевіряють її достовірність. Автор повинен розглянути, чи відповідає інформація формальним інформаційним вимогам партнера, чи може вона мати цінність для ширшої спільноти об'єктів критичної інфраструктури. Для дуже невеликих організацій цей крок може відбуватися неформально і одночасно з кроками 1 і 2, описаними вище.

[37] Докладнішу інформацію можна знайти на сайті https://www.us-cert.gov/tlp. Окрім US-CERT та інших національних спільнот фахівців з кібербезпеки, TLP також працює з організаціями державного та приватного сектору в Австралії, Канаді, Фінляндії, Франції, Німеччині, Угорщині, Італії, Японії, Нідерландах, Новій Зеландії, Норвегії, Швеції, Швейцарії та Сполученому Королівстві.

[38] TLP не поширюється на секретну інформацію. Програма "Контрольованої несекретної інформації" (CUI) спрямована на стандартизацію того, як виконавчі відомства та агентства США поводяться з чутливою, але несекретною інформацією(SBU), включаючи інформацію з грифом "Для службового користування" (FOUO), "Конфіденційна інформація для правоохоронних органів" (LES) та ін. Слід зазначити, що позначення TLP не є категорією або підкатегорією в рамках програми CUI.

Крок 4: Ініціатор надає інформацію відповідно до обмежень доступу та використання

Відповідно до рішень щодо захисту, прийнятих на Кроці 2, автор визначає, хто має право знати інформацію, створену згідно з відповідними законами та нормативними актами. Багато організацій, у тому числі ІС федерального уряду, правоохоронні органи, ISACs та ISAOs, встановлюють стандартні протоколи для маркування та поводження з інформацією. Автор може надавати інформацію через неформальні мережі (наприклад, з вуст в уста, електронні листи колегам, телефонні дзвінки або звичайні зустрічі), а також через офіційні канали, в тому числі, коли автор ділиться інформацією з хабом[39] для дискретного або ширшого розповсюдження.

- Формат:
  - Формат і зміст інформації, якою обмінюються, залежать від джерела та характеру інформації.
  - Якщо ІС має інформацію, яка може бути передана приватному сектору,[40] продукти надсилаються до FBI та DHS з відповідними грифами секретності на різних рівнях класифікації, включно з несекретними, якщо це можливо, щоб FBI та/або DHS могли розробити продукти, орієнтовані на конкретну аудиторію.
  - Інформація, отримана від приватного сектору або місцевих чи державних правоохоронних органів, може бути "знезаражена" відповідно до кроку 2.
  - Офіційні аналітичні продукти, як правило, не готуються до надсилання до хабів. Винятки можуть бути, якщо автором є галузеве відомство (SSA), дуже велика столична правоохоронна організація або дуже велика компанія з аналітичними кадрами.
- Механізми обміну:
  - Зазвичай інформація надсилається до центрів обміну інформацією через захищені електронні механізми, такі як Інформаційна мережа національної безпеки - критична інфраструктура (HSIN-CI), якою керує Міністерство внутрішньої безпеки США (DHS).[41]
  - Обмін інформацією може також відбуватися шляхом проведення особистих брифінгів або спільних конференц-дзвінків. Наприклад, Управління захисту інфраструктури (IP) Міністерства безпеки США і Міжгалузева рада (ради) Партнерства з безпеки критичної інфраструктури розробили документ "*Координаційний план цільової взаємодії з питань загроз і безпеки"*, в якому описано процес обміну інформацією між IP і CSCs.[42] План визначає процедури проведення цільових заходів, спрямованих на отримання розвідувальної інформації та інформації з питань безпеки щодо фізичних та кіберзагроз.
  - Обмін секретною інформацією повинен здійснюватися через канали та механізми, затверджені для обміну секретною інформацією.

[39] Розділ 3 "Описи суб'єктів обміну інформацією про загрози" містить описи різних центрів обміну інформацією, до яких належать урядові операційні центри, центри об'єднання штатів і великих міських районів, ISAC та ISAO з офіційними центрами спостереження, а також правоохоронні органи, такі як DSAC FBI та InfraGard тощо.

[40] Для отримання додаткової інформації про те, як розвідувальне співтовариство федерального уряду отримує, аналізує і ділиться розвідувальною інформацією, див. Посібник з розвідки *Об'єднаної антитерористичної групи з оцінки для тих, хто першим реагує:* https://www.ise.gov/sites/default/files/Intelligence%20Guide%20for%20First%20Responders_web.pdf (дата звернення: 21 червня 2016 р.).

[41] Перелік механізмів обміну інформацією наведено в Додатку E.

[42] Для отримання додаткової інформації про План координації цільових операцій з протидії загрозам і забезпечення безпеки див. Додаток F.

- Автоматизований обмін інформацією між машинами стає все більш поширеним для прискорення обміну інформацією про загрози, особливо пов'язані з кіберзагрозами. Багато таких систем[43] використовують Trusted Automated eXchange of Indicator Information (TAXII) як переважний метод обміну інформацією з використанням мови Structured Threat Information eXpression (STIX) для створення автоматизованого, машинозчитуваного потоку інформації про загрози і безпеку, якою можна обмінюватися між галузями і групами в режимі, близькому до реального часу.[44] Детальнішу інформацію про методи обміну див. в описі сутностей у Розділі 3.

Крок 5: Хаби збирають, інтегрують, перевіряють, оцінюють та аналізують інформацію; виробляють та обмінюються продуктами

За своєю суттю, хаби знають про інформаційні потреби своїх партнерів чи клієнтів. Таким чином, вони можуть оцінити, чи потребує інформація додаткового аналізу і чи варто нею ділитися з іншими партнерами.

- Отримавши інформацію, хаби здійснюватимуть власну перевірку та аналіз - інтегруватимуть нову інформацію з іншими знаннями та визначатимуть, чи варто її передавати іншим партнерам, і якщо так, то як адаптувати для їхнього використання.
- Якщо буде прийнято рішення надати інформацію іншим партнерам, хаб може провести додатковий аналіз і випустити офіційний продукт. (Типи продуктів можуть відрізнятися залежно від хабу та вимог клієнтів або зацікавлених сторін).
- Захисні заходи можуть бути переглянуті у світлі інтеграції, аналізу та цільової аудиторії продукту.
- Інформація надається партнерам хабу, серед яких можуть бути й інші хаби, за допомогою різних механізмів (наприклад, захищених веб-порталів, які дозволяють розміщувати інформацію або розвідувальні бюлетені, прямих телефонних дзвінків один на один, конференц-зв'язку, брифінгів і т.д.).

Крок 6: Мінімізація загрози

Співтовариство критичної інфраструктури отримує інформацію і приймає тактичні, оперативні та стратегічні рішення, щоб допомогти зменшити загрозу. Типи вжитих заходів залежать від ролей та обов'язків суб'єкта. Наприклад, власники та оператори можуть приймати тактичні рішення щодо посилення своїх захисних заходів, тоді як асоціації або програмні та політичні організації можуть розробити нові тренінги для розгортання по всій країні.

Крок 7: Цикл зворотного зв'язку

Важливою складовою циклу обміну інформацією є зворотний зв'язок, який одержувачі інформації надають авторам і виробникам аналітичних продуктів для покращення їхньої актуальності, корисності та формату.

---

[43] Прикладами міжмашинного обміну інформацією є Посилені послуги з кібербезпеки (Enhanced Cybersecurity Services, ECS), що пропонуються Міністерством безпеки США; Система подій безпеки і її компонент Колективної системи розвідки (Collective Intelligence Framework) від Центру обміну та аналізу інформації про науково-освітні мережі (Research and Education Networking Information Sharing and Analysis Center, REN-ISAC); а також Управління подіями з інформаційної безпеки в регіоні (Public Regional Information Security Event Management, PRISEM) від штату Вашингтон.

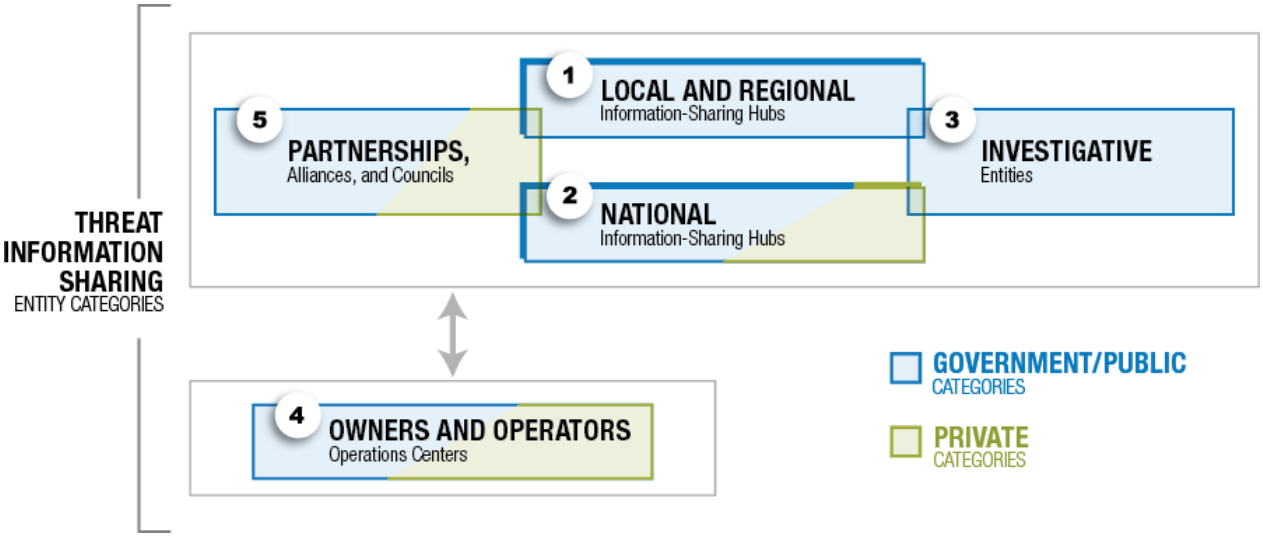
[44] Для отримання додаткової інформації див. http://measurablesecurity.mitre.org/docs/stix-intro-handout.pdf та https://www.oasis-open.org/news/pr/oasis-advances-automated-cyber-threat-intelligence-sharing-with-stix-taxii-cybox (датазвернення: 21 червня 2016 року).

Незалежно від того, чи є обмін інформацією вертикальним (між федеральним урядом та суб'єктами SLTT, власниками та операторами) або горизонтальним (наприклад, власники та оператори з власниками та операторами/штат зі штатом тощо), вживаються загальні заходи для визначення того, чим обмінюються, з ким, коли і як. Зокрема, роль центрів обміну інформацією, таких як операційні центри федерального уряду, InfraGard, об'єднані центри та ISAC, має вирішальне значення для ефективного та результативного обміну інформацією з приватним сектором. (Перелік та опис різних центрів обміну інформацією наведено в розділі 3). Ці центри також допускають і визнають, що неформальні мережі та особисті стосунки є необхідною і важливою частиною ефективного обміну інформацією про загрози з приватним сектором.

Використання центрів обміну інформацією дозволяє інтегрувати власників та операторів об'єктів критичної інфраструктури, а також партнерів з приватного сектору, що займаються питаннями безпеки, в екосистему обміну інформацією про загрози. Крім того, завдяки встановленим стандартам використання, обмеження доступу та інформаційної безпеки, партнери сектору можуть бути впевнені, що цілісність і конфіденційність їхньої конфіденційної інформації може бути і буде захищена, і що процес обміну інформацією може дати інформацію про загрози, яка може бути використана для вжиття відповідних заходів.

2.2 Типи організацій, що беруть участь у процесі обміну інформацієюпро загрози

Широку екосистему обміну інформацією про загрози та схожі ролі і обов'язки різних суб'єктів можна розділити на категорії відповідно до ролей, які вони відіграють у процесі обміну інформацією. Деякі зі згаданих суб'єктів підпадають під більш ніж одну категорію. Наведена нижче категоризація суб'єктів обміну інформацією про загрози не є новою політикою і не змінює існуючі відносини.



Малюнок 4: Категорії суб'єктів обміну інформацією про загрози

Перша і друга категорії (проілюстровані на малюнку 4) - це центри обміну інформацією, які узагальнюють отриману інформацію про загрози, а потім надають її своїм партнерам.
Вони беруть участь і часто сприяють як вертикальним, так і горизонтальним інформаційним потокам. Вони часто є оперативними центрами, аналітичними центрами або центрами спостереження. Багато з них працюють в режимі 24/7. Інші три категорії "Розслідування", "Власники та оператори" та "Партнерства" включені для того,щоб показати, як вони взаємодіють з центрами обміну інформацією та процесом обміну інформацією.

Далі в цьому розділі наведено приклади організацій у кожній категорії, а в Розділі 3 - опис окремих організацій, які, на думку робочої групи, є найбільш важливими для власників та операторів у контексті обміну інформацією про загрози.

ОНЛАЙН-ПЛАТФОРМИ

Ця Рамкова програма та категорії в цьому розділі зосереджені на суб'єктах, що обмінюються інформацією про загрози. Онлайн-платформи обміну інформацією, такі як HSIN, також відіграють важливу роль у процесі обміну інформацією про загрози і включені до опису організації, яка ними керує (наприклад, інформація про HSIN-CI включена до опису організації NICC). Невичерпний перелік відповідних платформ для обміну інформацією про загрози наведено в Додатку E: Механізми та джерела обміну інформацією про загрози та інструменти для оцінки загроз.

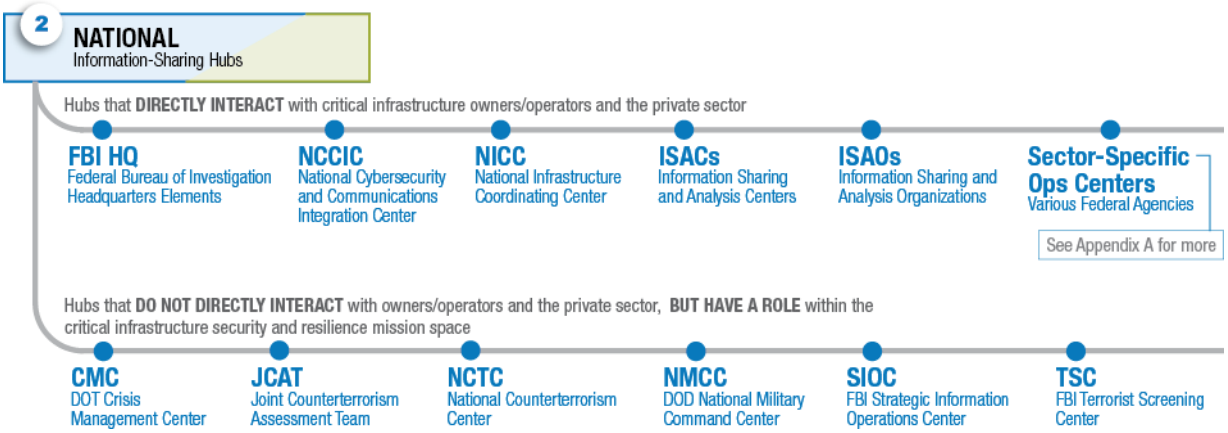
2.2.1 Місцеві та регіональні центри обміну інформацією

Місцеві та регіональні центри обміну інформацією працюють на місцевому або регіональному рівні, обслуговуючи переважно місцеве або регіональне коло клієнтів. Вони мають зв'язки з національними центрами і часто слугують каналом зв'язку між власниками та операторами і центральними офісами федеральних урядових установ. Ці організації представляють як державні та місцеві органи влади, так і федеральний уряд.

Малюнок 5: Місцеві та регіональні центри обміну інформацією

2.2.2 Національні центри обміну інформацією

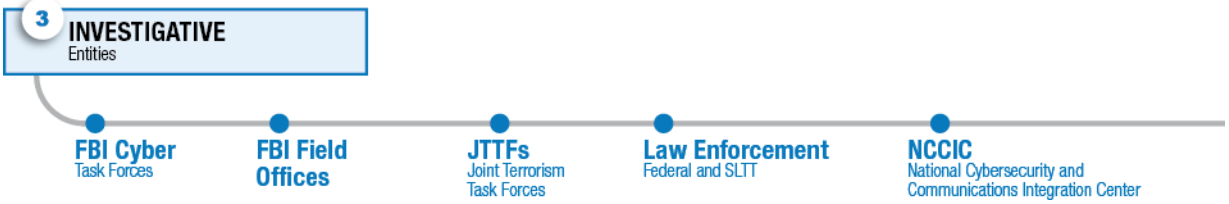
Національні центри обміну інформацією - це оперативні, аналітичні та/або спостережні центри, що відповідають за національну перспективу. У деяких випадках продукти, які вони створюють, поширюються через місцеві або регіональні центри обміну інформацією. Багато з цих організацій мають набагато ширшу місію, ніж забезпечення безпеки та стійкості критичної інфраструктури.[45]



Малюнок 6: Національні центри обміну інформацією

2.2.3 Слідчі органи

Слідчі органи не є в першу чергу "публічними". Їхнє головне завдання - проводити розслідування для правоохоронних органів. Як правило, слідчі органи не працюють і не обмінюються інформацією з власниками та операторами, за винятком випадків, коли вони проводять брифінги щодо загроз або розслідують конкретні питання, що стосуються власника або оператора. Однак вони можуть отримувати підказки або повідомлення про підозрілу діяльність від власників або операторів об'єктів критичної інфраструктури. Під час проведення розслідування інформація не передається широкій громадськості в рамках вищеописаного процесу. Якщо в ході розслідування виявляється, що інформація про загрозу потребує поширення, вона обробляється і розміщується в аналітичному звіті та бюлетені, а також поширюється серед відповідної аудиторії. Продукти, які вони виробляють, можуть поширюватися через організації інших категорій.



Малюнок 7: Слідчі органи

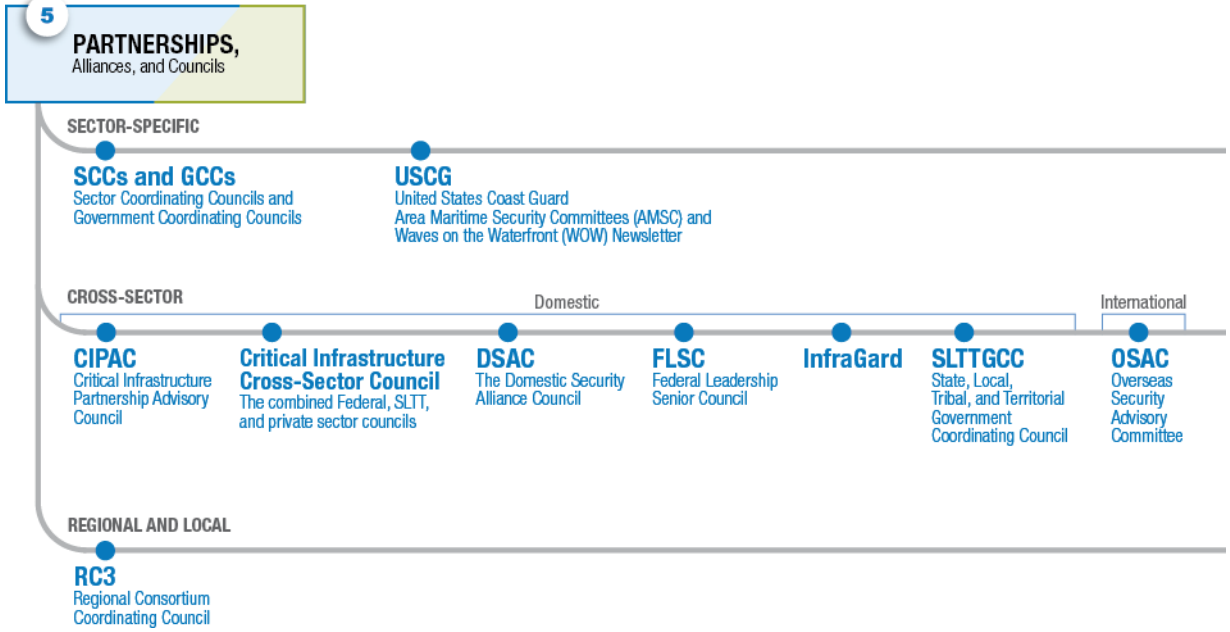
[45] Наприклад, членами Об'єднаної групи з антитерористичної оцінки (JCAT) є співробітники Служби швидкого реагування та фахівці з громадської безпеки з усієї країни, які працюють пліч-о-пліч з аналітиками федеральної розвідки з Національного антитерористичного центру (NCTC), Міністерства внутрішніх справ (DHS) та FBI над дослідженням, підготовкою та поширенням антитерористичної інформації. Місія JCAT полягає в поліпшенні обміну інформацією та підвищенні громадської безпеки. JCAT співпрацює з іншими членами IC з метою дослідження, виробництва та розповсюдження контртерористичних розвідувальних продуктів для федеральних і спеціальних урядових установ та приватного сектору, а також відстоює вимоги та потреби цих партнерів у контртерористичній розвідці в рамках IC.

2.2.4 Власники та оператори Операційних центрів

Оперативні центри безпеки власників та операторів управляються окремими суб'єктами критичної інфраструктури і, як правило, зосереджені на моніторингу та захисті активів цих суб'єктів. Однак функції цих центрів значно відрізняються між собою, і деякі з них можуть обмінюватися інформацією про загрози з іншими суб'єктами у своєму секторі, географічному регіоні тощо.

2.2.5 Партнерства, альянси та ради

Партнерства, альянси, ради та асоціації, серед іншого, сприяють співпраці та діалогу між своїми членами і часто надають механізми обміну інформацією (наприклад, портали, інструменти та брифінги) для використання їхніми членами. До цих організацій часто звертаються за експертними знаннями та/або використовують їх для швидкого надання інформації про загрози своїм членам в умовах підвищеної загрози або під час інциденту.



Малюнок 8: Партнерства, альянси та ради

Описи об'єктів обміну інформацією про загрози

Суб'єкти обміну інформацією про загрози, перелічені в цьому розділі, - це ті, що були визначені в процесі розробки Рамкової програми як такі, що відіграють певну роль у процесі обміну інформацією про загрози, описаному в Розділі 2. Інші відповідні суб'єкти, які не включені до Розділу 3, перераховані в Додатках А і Б, хоча Додатки не містять вичерпного переліку всіх суб'єктів, які обмінюються інформацією про загрози. Ці описи були складені самими організаціями на основі стандартної анкети.

Рада Альянсу з питань внутрішньої безпеки (DSAC)	
Категорія:	Партнерства, альянси та ради - Міжгалузеві - Внутрішні
Загальний опис:	DSAC - це очолюване FBI партнерство між Міністерством внутрішньої безпеки, федеральним урядом та компаніями зі списку Fortune 500 з метою зміцнення національної безпеки та зменшення ризиків для приватного сектору шляхом співпраці та обміну інформацією. Членство в DSAC охоплює 13 з 16 секторів критичної інфраструктури (сектори гребель, ядерної енергетики та урядових об'єктів наразі не охоплені). Інформація, що надається членам DSAC, призначена лише для членів DSAC, як це узгоджено кожним членом у Статуті членства DSAC.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури (специфічні для членів DSAC):	• Через свій портал, доступний лише для членів, DSAC поширює своєчасні, актуальні та дієві розвідувальні дані, які допомагають захистити критично важливу інфраструктуру нашої країни від терористів, злочинців та інших осіб чи груп, які становлять загрозу. • Вона створює мости між приватним сектором і місцевими відділеннями FBI, прагнучи сприяти конструктивному діалогу про ризики, з якими стикається кожна компанія окремо, про те, які ризики можуть мати тенденції на місцевому рівні або в певному секторі бізнесу, а також про те, як загроза може реалізуватися на національному рівні. • На додаток до свого порталу, доступного лише для членів, DSAC пропонує: ◦ Академію керівників з питань внутрішньої безпеки (для керівників служб безпеки компаній-членів DSAC)[46] ◦ Комплексні симпозіуми для аналітиків (для аналітиків компаній-членів DSAC)[47] ◦ Щорічні конференції DSAC (для CSOs компаній-членів DSAC)[48] ◦ Можливості нетворкінгу з іншими членами DSAC
Зверніться до DSAC, якщо:	• Ви є компанією зі списку Fortune 500 і хочете отримати членство • Як член DSAC, ви бажаєте отримати ресурси, включаючи індикатори, рекомендації, звіти, аналітичні продукти та тренінги • Як член DSAC, ви хочете поділитися тенденціями, тактикою, методами та процедурами (TTPs) або найкращими практиками
Як зв'язатися:	Для отримання доступу до веб-сайту та запиту на безпечний доступ, перейдіть за http://www.dsac.gov/.
DSAC в дії:	11 грудня 2015 року DSAC провів вебінар для своїх членів, щоб надати інформацію від FBI, DHS, Управління розслідувань національної безпеки (HSI), а також власників і операторів про потенційні терористичні, кримінальні та кіберзагрози, пов'язані з Суперкубком 50 і пов'язаними з ним заходами; огляд розкладу заходів і місць проведення Суперкубку на тиждень; а також огляд операцій з безпеки і міжвідомчого планування безпеки. Вебінар проводився за допомогою HSIN Connect, що дозволило учасникам приєднатися до нього за допомогою мобільного пристрою або стаціонарного комп'ютера.

[46] Академія керівників служб внутрішньої безпеки (DSEA) - це програма стратегічної взаємодії для керівників служб внутрішньої безпеки (CSOs) та вищого керівництва федеральних правоохоронних органів. DSEA проводиться двічі на рік в Академії FBI у Квантіко, штат Вірджинія, і є тижневою програмою. Серед учасників - представники CSOs, керівникиправоохоронних органів та відповідальні спеціальні агенти FBI на місцях. DSEA покликана забезпечити підготовку керівного складу та надати учасникам можливість обмінятися методологіями та передовим досвідом.

[47] Навчальна програма Integrated Analyst Symposium (IAS) - це чотириденна серія тренінгів, покликана надати аналітикам базові робочі знання зі структурованого аналізу. За допомогою лекцій та вправ у малих групах студенти отримують інструкції щодо структурованих аналітичних методів (SAT) для оцінки та підготовки аналітичних оцінок. Навчальна програма IAS починається з базової термінології, розвідувального циклу та сортування інформації. Потім учасники переходять до розділу, присвяченого упередженням та умонастроям, критичному мисленню та практичному застосуванню SAT. Навчання завершується прикладною вправою з аналізу, де студенти отримують зразок сценарію і повинні виявити ризик, визначити масштаби проблеми, проаналізувати наявні дані і розробити кілька варіантів дій, щобпредставити їх керівництву для інформування.

[48] Конференція DSAC - це панельні дискусії та обговорення за участю керівників FBI, Міністерства національної безпеки та лідерів приватного сектору. Дискусії охоплюють різноманітні сучасні проблеми, що стоять перед урядом і приватним сектором, від кібербезпеки до інсайдерських загроз і міжнародних викрадень.

Відділення FBI на місцях	
Категорія:	Місцеві та регіональні центри обміну інформацією; та слідчі органи
Загальний опис:	FBI має 56 місцевих відділень, розташованих у великих мегаполісах США та Пуерто-Рико, де FBI проводить розслідування, оцінює місцеві та регіональні кримінальні загрози, а також тісно співпрацює з федеральними партнерами та партнерами SLTT у справах та операціях. Оскільки FBI є провідним слідчим органом з питань тероризму та контррозвідки (згідно з Указом Президента № 12333), про всі загрози тероризму та контррозвідки слід повідомляти донайближчого місцевого відділення FBI безпосередньо або через місцеві органи влади (включно з об'єднаними центрами).
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	FBI має багато програм приватного сектору по всій країні. На додаток до DSAC (згаданої вище) та InfraGard (згаданої нижче), FBI також має інформаційних координаторів у кожному з 56 місцевих відділень, а також онлайн-ресурси для цих програм і не тільки: • Active Shooter: https://www.fbi.gov/about-us/office-of-partner-engagement/active-shooter-інциденти • Зв'язок з кампусом: https://www.fbi.gov/news/stories/2009/august/campussecurity_080409 • Програма "Робота з громадою": https://www.fbi.gov/about- us/partnerships_and_outreach/community_outreach • Стратегічне партнерство з контррозвідки: https://www.fbi.gov/about-us/partnerships_and_outreach/investigate/counterintelligence/strategic-partnerships • Альянс з кібер-криміналістики та навчання: https://www.fbi.gov/news/stories/2011/september/cyber_091611 • Брошура "Внутрішня загроза": https://www.fbi.gov/about- us/investigate/counterintelligence/insider_threat_brochure • Короткий огляд державно-приватних партнерств з обміну інформацією: https://www.fbi.gov/about- us/partnerships_and_outreach/ • Тероризм: https://www.fbi.gov/about-us/investigate/terrorism • Зброя масового знищення: https://www.fbi.gov/news/stories/2007/march/wmd030507 • FBI дотримується Директиви розвідувального співтовариства ODNI 191 "Обов'язок попереджати", підписаної 21.07.2015: http://www.dni.gov/files/documents/ICD/ICD_191.pdf
Зверніться до місцевого відділення FBI щоб:	• Повідомити про всі терористичні та контррозвідувальні загрози • Повідомити про кіберінцидент • Отримати продукт або послуги, як зазначено вище
Як зв'язатися:	Ви можете повідомити про загрози та інциденти і зв'язатися з найближчим відділенням: • Онлайн: https://www.fbi.gov/report-threats-and-crime • Зверніться до найближчого відділення FBI за адресою https://www.fbi.gov/contact-us/field або до найближчого міжнародного офісу за адресою https://www.fbi.gov/contact-us/legat • Щоб повідомити про підозрілу діяльність, пов'язану з хімічними, біологічними або радіологічними матеріалами, телефонуйте (безкоштовно) 855-TELL-FBI (855-835-5324) • Повідомте про шахрайство в Інтернеті або містифікацію електронної пошти, подавши скаргу до Центру розгляду скарг на злочини в Інтернеті за адресою http://www.ic3.gov/complaint/default.aspx або скориставшись онлайн-формою "Поради та повідомлення громадськості" за адресою https://tips.fbi.gov/. • Щоб надати інформацію про окремі великі справи, зателефонуйте до Контактного центру з великих справ за номером 1-800-CALL-FBI (1-800-225-5324).
Офіси FBI на місцях в дії:	Стрілянина на військово-морській базі у Вашингтоні, вибухи на Бостонському марафоні та ураган Сенді є прикладами великих справ і катастрофічних подій, про які FBI хоче почути від громадськості, щоб FBI могло швидко вжити заходів для надання допомоги, захисту та запобігання загрозам для цієї країни та її населення.

Федеральні галузеві операційні центри	
Категорія:	Національні центри обміну інформацією - багато взаємодіють з власниками/операторами[49]
Загальний опис:	Федеральні департаменти та відомства використовують свої організаційні операційні/наглядові центри для задоволення внутрішніх вимог щодо обміну інформацією, пов'язаної з безпекою критичної інфраструктури та ситуативною обізнаністю щодо стійкості. Ролі та обов'язки відповідних федеральних оперативних центрів, а також контактні особи перераховані в Додатку А.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Забезпечення ситуаційної обізнаності та обмін інформацією у випадку стихійного лиха, терористичного акту чи іншого лиха • Слугує щоденним федеральним інтерфейсом для динамічного визначенняпріоритетів, співпраці та координації галузевої діяльності • Захист критично важливої інфраструктури та забезпечення безперервності роботи уряду за допомогою процесу управління ризиками на основі стандартів Міжвідомчого комітету з безпеки та Національного плану захисту інфраструктури (NIPP) • Забезпечує попередження та/або припинення інцидентів, зменшення загроз, а також координацію та управління інцидентами • Сприяє безперервності операцій/управління, політики у сфері надзвичайних ситуацій, планування, підтримки та оперативної координації; а також спеціальних програм безпеки
Зверніться до Федерального оперативного центру щоб:	Ці операційні центри часто спілкуються безпосередньо з власниками та операторами у своєму секторі, хоча деякі з них спілкуються переважно під час катастроф.
Додаткова інформація:	у Додатку А наведено перелік федеральних галузевих операційних центрів, їхні функції, веб-сайти та контактна інформація.

[49] Федеральні галузеві операційні центри мають різні операційні моделі. Деякі з них переважно забезпечують внутрішні потреби відомства не взаємодіють безпосередньо з власниками та операторами об'єктів критичної інфраструктури, хоча багато хто з них взаємодіє. Для отримання додаткової інформації див. опис організацій у Додатку А.

Об'єднані центри (об'єднані центри штатів і великих міських районів)

Категорія:	Місцеві та регіональні центри обміну інформацією
Загальний опис:	Об'єднані центри штатів і великих міських районів належать і управляються державними і місцевими органами влади і служать основними координаційними центрами в межах штату і на місцевому рівні для отримання, аналізу, збору та обміну інформацією про загрози між федеральними органами влади, SLTT і партнерами з приватного сектору. Об'єднані центри надають міждисциплінарну експертизу щодо всіх видів злочинів і загроз, а також ситуаційну обізнаність, що допомагає приймати рішення на всіх рівнях влади і в приватному секторі. Вони проводять аналіз і сприяють обміну інформацією, допомагаючи правоохоронним органам і партнерам з національної безпеки запобігати, захищати і реагувати на злочинну діяльність, тероризм і загрози та реагувати на них.
Функції, продукти та послуги, що мають відношення до спільноти КІ:	Продукти об'єднаних центрів допомагають клієнтам зрозуміти місцеві наслідки національної розвідки, таким чином допомагаючи державним і місцевим органам влади краще захищати свої громади, а партнерам з приватного сектору - свої об'єкти та операції. Ці продукти часто надаються партнерам з приватного сектору безпосередньо з об'єднаного центру, і до багатьох продуктів можна отримати доступ через спільноту за інтересами "Інформаційна мережа з питань національної безпеки - КІ" (Homeland Security Information Network - Critical Infrastructure, HSIN-CI), яка полегшує обмін продуктами і інформацією з усіма партнерами-учасниками: https://www.dhs.gov/hsin-ci. Залежно від своєї спрямованості та індивідуальних потреб клієнтів, об'єднані центри можуть надавати кілька типів продуктів та послуг: • **Відповіді на інформаційні запити** - запит на отримання конкретної інформації від клієнта • **Продукти ситуаційної обізнаності** - інформація про події або інциденти, що розвиваються • **Бюлетені** - інформація про кримінальні загрози та інциденти та/або потенційнітерористичні загрози • **Попереджувальні бюлетені розвідки** - достовірні звіти або аналітичні вказівкина конкретну або неминучу загрозу • **Консультативні повідомлення** - інформація щодо регіональних інцидентів у сфері кібер- та фізичної безпеки, а також тенденцій і тактики розвитку злочинності • **Формальні звіти** - формалізовані періодичні та ситуаційні звіти • **Оцінки загроз** - детальна інформація про характер конкретної загрози, а також поточні та майбутні тенденції • **Оцінки ризиків** - комплексні оцінки, засновані на аналізі загроз,вразливостей та наслідків • Брифінги з питань засекречених загроз
Зверніться до Об'єднаного центру у вашому регіоні, щоб:	• Отримати інформацію про доступні продукти та послуги, способи доступу до них • Приєднатись до списків розсилки або порталів обміну інформацією в Інтернеті • Поділитися інформацією про повідомлення про підозрілу діяльність (SAR) з вашим регіональним об'єднаним центром по боротьбі з тероризмом та іншою пов'язаною з ним злочинною діяльністю (безкоштовний онлайн-тренінг з SAR для приватного сектору та інших секторів доступний за посиланням https://nsi.ncirc.gov/training_online.aspx). • Ділитися порадами та зачіпками щодо злочинів, не пов'язаних з тероризмом (не всі об'єднані центри займаються всіма видами злочинів) • Брати участь в управлінні об'єднаним центром або працювати в дорадчому органі • Зв'язатися з федеральним персоналом на місцях. У багатьох випадках FBI, DHS та інші відомства, що мають свої підрозділи на місцях, розміщують персонал в об'єднаних центрах або спільно з ними.
Як зв'язатися:	- Для отримання додаткової інформації про об'єднаний центр у вашому регіоні відвідайте https://www.dhs.gov/contact-fusion-centers. • Ви можете залучити персонал DHS, зокрема регіональних директорів з питань внутрішньої безпеки та аудиту, офіцерів розвідки та офіцерів з питань звітності, радників з питань безпеки. • Зверніться до офіцера зв'язку, відповідального за роботу з приватним сектором в об'єднаному центрі.
Об'єднані центри в дії:	Мають мережу контактів у всій зоні своєї відповідальності. Ця мережа дозволяє об'єднаним центрам звертатися до громадськості для збору інформації, яка може допомогти правоохоронним органам у розкритті злочинів або запобіганні терористичним атакам. Одним із прикладів є справа про запланований терористичний напад водія маршрутного таксі в аеропорту Денвера. Ф'южн-центр сприяв збору інформації з магазинівпостачання по всьому штату Колорадо. Аналіз зібраної інформації допоміг запобігти нападу і сприяти арешту терориста. Будь ласка, також ознайомтеся з прикладами використання в Розділі 4. Додаткові приклади використання можна знайти на сторінці успіху Об'єднаного центру на сайті DHS.gov: https://www.dhs.gov/fusion-center- success-stories.

Центри обміну та аналізу інформації (ISAC)	
Категорія:	Національні центри обміну інформацією - взаємодіють безпосередньо з власниками/операторами; та партнерства, альянси та ради - галузеві
Загальний опис:	ISAC - це галузеві, приватні, довірені організації, створені власниками та операторами критичної інфраструктури для збору, аналізу та розповсюдження своєчасної та дієвої інформації про загрози серед своїх членів, інших секторів та урядових установ. ISAC також надають своїм членам інструменти та найкращі практики для зменшення ризиківта підвищення стійкості. Залежно від сектору, ISAC можуть працювати на безоплатній або платній основі.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	Кожен ISAC використовує знання та досвід у своїй галузі: • Заощаджує час та зусилля членів, виступаючи в ролі інформаційного центру для урядової та приватної інформації, допомагаючи членам виявляти ризики, готуватися до надзвичайних ситуацій та захищати критично важливу інфраструктуру в конкретному секторі. • Досліджує та аналізує отриману інформацію, щоб підтвердити достовірність інформації та серйозність будь-яких загроз, а також надати рекомендації щодо дій. • Фільтрує інформацію за галузевими та регіональними специфікаціями • Повідомляє про загрози та звіти про інциденти через електронні розсилки, електронні листи з повідомленнями про загрози або іншими способами ◦ Надає членам організації інструменти для виявлення та управління ризиками ◦ Сприяє співпраці та комунікації між учасниками, використовуючи безпечну довірену мережу для підтримки їхньої взаємної вигоди
Зверніться до вашого ISAC сектору щоб:	• Дізнатися більше про можливості ISAC у вашому секторі • Приєднатись до ISAC вашого сектору • Повідомити про інцидент у конкретному секторі
Як зв'язатися:	Нижче наведено список ISAC за секторами/галузями та їхні веб-сайти • Веб-сайт Національної ради ISAC надає інформацію про міжсекторальну співпрацю та додаткову інформацію про кожну з ISAC: www.nationalisacs.org
ISAC в дії:	01.01.2016 експерти-аналітики Electricity ISAC (E-ISAC) оприлюднили для представників електроенергетичного сектору несекретний комплексний Звіт про кіберподії, в якому детально описані певні події грудня 2015 року в Україні. У цьому компілятивному продукті з відкритим вихідним кодом описано реальні події, надано детальну довідкову інформацію, застосовано галузевий аналіз з урахуванням впливу та пом'якшення наслідків для сектору та інших, надано технічну інформацію. В E-ISAC також відбулася наступна міжсекторальна зустріч аналітиків з федеральними партнерами для організацій-партнерів у сфері безпеки.
Веб-сайти ISAC:	- Авіація (A-ISAC): www.a-isac.com • Комунікації (COMM-ISAC):[50] http://www.dhs.gov/national-coordinating-center-communications • Оборонно-промислова база (DIB-ISAC): http://dibisac.net/ • Переробка та реалізація природного газу (DNG-ISAC): www.dngisac.com/ • Електроенергетика (E-ISAC): www.eisac.com • Служби з надзвичайних ситуацій (EMR-ISAC): www.usfa.fema.gov/fireservice/emr-isac • Фінансові послуги (FS-ISAC): www.fsisac.com • Охорона здоров'я (NH-ISAC): www.nhisac.org • Інформаційні технології (IT-ISAC): www.it-isac.org • Багатодержавний (MS-ISAC): www.msisac.org • Nuclear (NEI): www.nei.org/ • Нафта і природний газ (ONG-ISAC): www.ongisac.org/ • Громадський транспорт (PT-ISAC): www.surfacetransportationisac.org • Нерухомість (RE-ISAC): www.reisac.org • Дослідницька та освітня мережа (REN-ISAC): www.ren-isac.net • Центр обміну розвідувальною інформацією в сфері роздрібної торгівлі (RCS-ISAC): http://r-cisc.org/ • Ланцюг постачання (SC-ISAC): www.sc-isac.org • Наземний транспорт (ST-ISAC): www.surfacetransportationisac.org • Вода (WaterISAC): www.waterisac.org • Healthcare Ready www.healthcareready.org

[50] Національний координаційний центр зв'язку NCCIC (NCC) виконує функції COMM-ISAC.

Організації з обміну та аналізу інформації (ISAOs)	
Категорія:	Місцеві, регіональні та національні центри обміну інформацією - взаємодіє безпосередньо з власниками/операторами; а також партнерства, альянси та ради
Загальний опис:	ISAO - це ширша категорія приватних організацій з обміну інформацією, до яких належать ISACs. Деякі організації не вписуються у визначений сектор або мають унікальні потреби. Ті організації, які не можуть приєднатися до ISAC, але мають потребу в інформації про загрози, можуть отримати вигоду від членства в ISAO, наприклад, культові споруди. Створення нових ISAO дозволяє зацікавленим спільнотам обмінюватися інформацією про загрози один з одним і з існуючими державними і приватними організаціями на добровільних засадах для створення більш глибоких і широких мереж обміну інформацією про загрози в масштабах всієї країни. Президент Обама видав указ, яким доручив Міністерству внутрішніх справ заохочувати розробку нових стандартів ISAO, а Організація стандартів ISAO (ISAO-SO), очолювана Техаським університетом у Сан-Антоніо, з моменту свого заснування 01.10.2015 працює зі спільнотою КІ над визначенням спільного набору добровільних стандартів для створення та функціонування ISAO. Ці стандарти є однією зключових відмінностей між ISAO та ISAC.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Кожна ISAO використовує свої галузеві знання та досвід: • Виконує роль інформаційного центру для обміну інформацією про загрози з боку уряду та приватних осіб, що допомагає членам організації виявляти ризики, готуватися до надзвичайних ситуацій та захищати критично важливу інфраструктуру. • Досліджує та аналізує отриману інформацію, щоб підтвердити її точність та серйозність, а також рекомендує дії • Фільтрує інформацію за галузевою та регіональною специфікацією • Повідомляє про загрози та звіти про інциденти через електронні розсилки, електронні листи з повідомленнями про загрози або іншими способами ◦ Надайте інструменти для виявлення та управління ризиками ◦ Сприяти співпраці та комунікації між членами для їхньої взаємної вигоди ◦ Розширювати взаємовідносини спільного використання за межі традиційних секторів критичної інфраструктури, наприклад, місця відправлення культу.
Зв'яжіться з відповідними ISAO або Організацією зі стандартизації ISAO (ISAO-SO) щоб:	• Дізнатися більше про те, що передбачають відповідні ISAO • Приєднатися до ISAO • Запустити новий ISAO • Повідомити про інцидент у конкретному секторі
Як приєднатися:	- ISAO є новим типом організацій, і на момент написання цієї статті вони ще не існують у повномуобсязі • Дізнайтеся більше про ISAO на сайті http://www.dhs.gov/isao • Ознайомитися з інформаційним бюлетенем ISAO можна за посиланням https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet- executive-order-promoting- private-sector-cybersecurity-inform • Щоб взяти участь у розробці або отримати доступ до стандартів і настанов для започаткування нових ISAO, відвідайте Організацію зі стандартизації ISAO за адресою https://www.isao.org або напишіть на електронну пошту contact@isao.org.

InfraGard	
Категорія:	Партнерства, альянси та ради - Міжгалузеві - Внутрішні
Загальний опис:	InfraGard - це державно-приватне партнерство між FBI та понад 40 000 перевірених представників приватного сектору, які представляють усі 16 секторів критичної інфраструктури. Це об'єднання членів, які мають профільну експертизу і представляють бізнес, наукові установи, уряди всіх рівнів, державні та місцеві правоохоронні органи, а також інші учасники, покликані забезпечити багатовекторний обмін інформацією, розвідданими, стратегіями та досвідом для запобігання ворожим діям проти США. По всійкраїні налічується понад 80 відділень InfraGard.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Члени InfraGard мають доступ до: • Безпечного веб-порталу InfraGard для обміну інформацією • iGuardian, інструменту FBI для повідомлення про кіберінциденти, розроблений спеціально для приватного сектору • Комплексного набіру чутливих, несекретних розвідувальних проектів FBI та інших загроз, а також щоденні стрічки новин з багатьох джерел • Попередження про загрози від FBI та DHS, бюлетені розвідки, аналітичні звіти та оцінки вразливостей в режимі реального часу ◦ Заходи, організовані місцевими альянсами-членами InfraGard (IMA), які включають презентації FBI та інших урядових установ і надають можливість особистого спілкування та обміну інформацією про загрози в довірливому середовищі. ◦ Забезпечення місця, якщо необхідно, для повідомлення про загрози та їх обговорення ◦ Навчання
Зв'яжіться з InfraGard, щоб:	- Стати учасником (Ви повинні бути громадянином США і мати 18 років або більше) • Попросіть про брифінг або тренінг у місцевому представництві IMA • Повідомте про кібервторгнення через захищений портал InfraGard, iGuardian (лише для членів InfraGard) ◦ Будь-хто може повідомити про кіберінцидент до Центру FBI зі скарг на інтернет-злочинність (IC3): http://www.ic3.gov
Як зв'язатися:	- Заявка на членство та доступ до захищеного веб-порталу InfraGard: www.infragard.org • Із загальними питаннями щодо членства, будь ласка, звертайтеся за адресою: questions@infragardmembers.org
InfraGard в дії:	З 27.02.2015 Malware Investigator вперше став доступним для приватного сектору через портал InfraGard для учасників програми. Malware Investigator використовує широке поєднання інструментів динамічного і статичного аналізу, щоб зрозуміти, як зразки шкідливого програмного забезпечення взаємодіють в різних типах хост-середовищ. Платформа також корелює зразки і дозволяє співпрацювати з іншими, за бажанням, щоб "з'єднати точки" між кіберподіями. Система, створена у співпраці з федеральними партнерами, є розширенням внутрішнього інструменту аналізу шкідливого програмного забезпечення, який FBI створило для власного використання в 2011 році. Доступ приватних партнерів до Malware Investigator приносить користь як приватним партнерам, так і FBI, зміцнюючи стратегічне партнерство через співпрацю, що в кінцевому підсумку допоможе зрозуміти загрози шкідливого програмного забезпечення та боротися з ними.

Слідчі та/або розвідувальні органи (непублічні)	
Категорія:	Слідчі органи
Загальний опис:	За багатьма публічними федеральними установами, що обмінюються інформацією про загрози, стоїть багато інших непублічних федеральних слідчих органів, які обмінюються інформацією в рамках федерального уряду.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	Розвідувальні продукти або похідні від них передаються власникам і операторам через інші організації, перелічені в цій Рамковій програмі.
Контакт:	Ці операційні центри зазвичай не спілкуються безпосередньо з власниками та операторами.
Як зв'язатися:	Для отримання додаткової інформації див. Посібник з розвідки для осіб, які першими реагують, від Об'єднаної групи з оцінки контртерористичних заходів (JCAT): http://www.nctc.gov/jcat/docs/Intelligence_Guide_for_First_Responders.pdf
Оберіть слідчі та/або розвідувальні органи (непублічні):	**Об'єднана антитерористична група (JTTF):** JTTF слугують скоординованою "зброєю" для федеральних, штатних і місцевих органів влади для розслідування терористичних загроз у певних географічних регіонах США. FBI є провідним відомством, яке здійснює нагляд за діяльністю JTTF. Місія JTTF полягає у використанні колективних ресурсів агентств-членів для запобігання, попередження, стримування і розслідування терористичних актів, що зачіпають інтереси США; для зриву і запобігання терористичним актам; а також для затримання осіб, які можуть вчинити або планують вчинити такі акти. З метою сприяння виконанню цієї місії, JTTF сприяє обміну інформацією між членами JTTF. Понад 500 державних і місцевих агентств беруть участь у роботі JTTF по всій країні, а федеральне представництво включає учасників з IC, DHS, а також міністерств оборони, юстиції, фінансів, транспорту, торгівлі, енергетики, державного департаменту і внутрішніх справ, серед інших.[51] **Національний контртерористичний центр (NCTC):** NCTC є головною організацією у федеральному уряді з інтеграції та аналізу всіх розвідувальних даних, що стосуються тероризму, якими володіє або які отримує федеральний уряд (за винятком суто внутрішнього тероризму); служить центральним і спільним банком знань про тероризм; надає розвідувальну підтримку загальнодержавній антитерористичній діяльності з усіх джерел; і забезпечує інтеграцію, розповсюдження та використання інформації про тероризм.[52] Він також видає Антитерористичний дайджест NCTC, збірник міжнародних і національних новин, присвячений інформації про боротьбу з тероризмом. Він доступний на сайтах HSIN-CI, InfraGard і DSAC. CT Дайджест також містить оцінки від досвідчених аналітиків і фахівців, які першими реагують на тероризм. **Центр скринінгу терористів (FBI-TSC):** Створений у 2003 році після подій 11 вересня, TSC веде консолідований список терористів - єдину базу даних ідентифікаційної інформації про осіб, які відомі або обґрунтовано підозрюються у причетності до терористичної діяльності. Підтримуючи здатність агентств, що здійснюють перевірку на передовій, позитивно ідентифікувати відомих або підозрюваних терористів, які намагаються отримати візи, в'їхати в країну, сісти на борт літака або займатися іншою діяльністю, зведений список терористів є одним з найефективніших інструментів боротьби з тероризмом для американського уряду.

[51] Національний антитерористичний центр, Посібник з розвідки JCAT для осіб, які здійснюють перше реагування, http://www.nctc.gov/jcat/docs/Intelligence_Guide_for_First_Responders.pdf (дата звернення: 21 червня 2016 р.).

[52] Національний антитерористичний центр, Хто ми є, http://www.nctc.gov/whoweare.html (дата звернення: 21 червня 2016 р.).

Місцеві та штатні оперативні центри правоохоронних органів	
Категорія:	Місцеві та регіональні центри обміну інформацією; та слідчі органи
Загальний опис:	У надзвичайних ситуаціях завжди телефонуйте 9-1-1, щоб зв'язатися з місцевими або державними правоохоронними органами. Системи обміну інформацією про загрози та розвідувальну інформацію між правоохоронними органами різняться залежно від громади. Деякі великі міста створили довірливі, усталені відносини з обміну інформацією і механізми, в той час як в інших власникам і операторам може бути складно регулярно спілкуватися з поліцією про підозрілу активність. Наприклад, Департамент поліції Нью-Йорка (NYPD) спонсорує сповіщення електронною поштою, веб-брифінги та періодичні особисті брифінги. Їхній штат аналітиків спеціально займається запобіганням тероризму і поширює інформацію в приватному секторі, і в рази швидше аналізує і поширює інформацію, ніж HSIN-CI. Однак ця мережа доступна лише для об'єктів критичної інфраструктури в Нью-Йорку.[53] Іншим прикладом є Автоматизований довірений обмін інформацією (ATIX) Регіональних систем обміну інформацією (RISS), групи спільнот якого включають правоохоронні органи, управління надзвичайними ситуаціями, уряд, а також зростаючу кількість груп, що перетинаються з критично важливими секторами інфраструктури, включаючи водо- та електропостачання, транспорт, сільське господарство, хімічне виробництво, приватну безпеку, охорону навколишнього середовища, банківську справу та фінанси, а також готельний бізнес.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Екстрене реагування на фізичні та кіберзагрози та інциденти, підтримка у разі їхвиникнення • Обмін інформацією про загрози • Розслідування інцидентів
Зверніться до місцевого оперативного центру правоохоронних органів щоб:	• Вивчити можливості для співпраці та обміну інформацією про місцеві загрози • Підписатися на сповіщення про загрози та інші послуги, які можуть бути доступні
Як зв'язатися:	- Зверніться до місцевих правоохоронних органів за номером телефону, відмінним від 911 • Приклад веб-порталу: Департамент поліції Нью-Йорка: http://www.nypdshield.org/public/ • RISS ATIX: Більше інформації, включаючи контактну інформацію регіональних центрів, можна знайти в брошурі, розміщеній на сайті www.riss.net/Resources/ATIX.

[53] Національна консультативна рада з питань інфраструктури, *Обмін розвідувальною інформацією: Заключний звіт та рекомендації*, січень 2012 р., http://www.dhs.gov/sites/default/files/publications/niac-intel-info-sharing-final-report-01-10-12- 508.pdf (дата перегляду: 21 червня 2016 р.), p. D-10.

Національний центр інтеграції кібербезпеки та комунікацій (NCCIC)	
Категорія:	Національні центри обміну інформацією - взаємодіють безпосередньо з власниками/операторами та слідчими органами
Загальний опис:	NCCIC слугує координаційним центром для координації інцидентів у сфері кібербезпеки, обміну інформацією та реагування на інциденти у федеральному цивільному уряді, а також надає партнерам з державного та приватного секторів допомогу у сфері кібербезпеки та національної безпеки/готовності до надзвичайних ситуацій у сфері комунікацій. Ці послуги включають захист, запобігання, виявлення, пом'якшення наслідків, реагування та, у випадку комунікацій, послуги з відновлення. Партнерами NCCIC є всі федеральні міністерства і відомства, уряди СЛТТ, приватний сектор, розвідувальне співтовариство, правоохоронні органи і міжнародні організації. NCCIC складається з 4 підрозділів: Команди готовності до комп'ютерних надзвичайних ситуацій США (US-CERT), Команди реагування на кібернетичні надзвичайні ситуації в промислових системах управління (ICS-CERT), Національного координаційного центру зв'язку (NCC) та Оперативно-інтеграційного підрозділу, до складу якого входить Національна служба оцінки та технічної підтримки кібербезпеки (NCATS). Для отримання додаткової інформації про кожну гілку див. https://www.dhs.gov/cyber-incident-response.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Обмін інформацією: ◦ Особистий обмін інформацією на вахтовому поверсі NCCIC ◦ Двосторонній обмін дієвими індикаторами кіберзагроз через два захищених веб-портали та через захищений міжмашинний інтерфейс "Автоматизований обмін індикаторами" (AIS): ◦ Програма обміну кіберінформацією та співробітництва (CISCP) ◦ Автоматизований обмін та отримання індикаторів кіберзагроз у машинозчитуваному форматі, відомому як Structured Threat Information eXpression (STIX) ◦ Обмін інформацією в міру необхідності через постійні групи ◦ Широке розповсюдження сповіщень, брифінгів, порад та бюлетенів, що мають практичне значення, серед спільноти за допомогою різних засобів, включаючи електронну пошту, два захищених веб-портали, ISAC та SSA. • Координація та управління національним реагуванням на значні кіберінциденти та надання безпосередньої допомоги жертвам кібератаки за запитом • Координує зусилля зі зниження ризиків, працюючи безпосередньо з власниками та операторами: ◦ Безкоштовні, виїзні, поглиблені оцінки кібербезпеки об'єктів критичної інфраструктури, які допомагають власникам і операторам підготуватися до кібератак і захиститися відних ◦ Безкоштовне навчання для покращення навичок та практик кібербезпеки власників активів ◦ Аналіз шкідливої активності ◦ Послуги з реагування на інциденти • Сприяння робочим групам, які обмінюються ідеями щодо методів пом'якшення наслідків
Зверніться до NCCIC за адресою:	• Повідомити про підозру або підтверджений кіберінцидент54 • Отримуйте ресурси з кіберзахисту, включаючи індикатори, попередження про загрози,звіти та дайджести шкідливого програмного забезпечення, призначені для власників та операторів об'єктів критичної інфраструктури • Отримати стратегії щодо запобігання, захисту та пом'якшення наслідків • Замовте та заплануйте безкоштовну виїзну оцінку кібербезпеки ваших систем управління, ресурсів та доступності на місці • Дізнайтеся, як подавати індикатори кіберзагроз до DHS, якими можна ділитися з іншими суб'єктами приватного сектору для покращення їхнього мережевого захисту, в тому числі за допомогою автоматизованого обміну індикаторами (AIS): www.us-cert.gov/ais

[54] Для отримання додаткової інформації про те, коли, про що і як повідомляти про кіберінциденти федеральномуряду, див. https://www.dhs.gov/sites/default/files/publications/Law%20Enforcement%20Cyber%20Incident%20Reporting.pdf (дата звернення 21.06.2016)

Національний центр інтеграції кібербезпеки та комунікацій (NCCIC)

Як зв'язатися:	:- Щоб повідомити про інцидент, відвідайте веб-сайт https://www.us-cert.gov/forms/report, напишіть на електронну пошту nccic.customerservice@hq.dhs.gov або зателефонуйте за номером888-282-0870 • Щоб повідомити про кіберінциденти, спрямовані на промислові системи управління, пишіть на ics-cert@hq.dhs.gov або телефонуйте за номером 877-776-7585 • Щоб отримувати сповіщення NCCIC, зареєструйтеся на сайті https://www.us-cert.gov/mailing-lists-and-feeds. • Щоб взяти участь в автоматизованому обміні індикаторами, перейдіть за посиланням https://www.us-cert.gov/ais • Щоб подати запит на проведення різних оцінок кібербезпеки, перейдіть за посиланням https://www.us-cert.gov/ccubedvp/assessments або https://ics-cert.us-cert.gov/Assessments, або напишіть на електронну пошту ncats_info@hq.dhs.gov. • Подати запит на безпечний доступ до порталу: ◦ US-CERT Cobalt Compartment (корпоративні системи) - щоб отримати доступ, надішліть електронного листа на адресу NCCIC_Partnership@hq.dhs.gov з темою листа "Request access to Cobalt Compartment". ◦ Відділ систем управління ICS-CERT (власники та оператори ICS) - для запиту доступу надішліть електронний лист на адресу ics-cert@hq.dhs.gov з темою листа "Запит надоступ до відділу систем управління". ◦ Для отримання додаткової інформації відвідайте https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
NCCIC в дії:	див. приклад використання Havex/BlackEnergy в Розділі 4.1, щоб дізнатися, як NCCIC ділився інформацією про загрози шкідливого програмного забезпечення ICS з власниками та операторами за допомогою брифінгів та сповіщень.

Національний інфраструктурний координаційний центр (NICC)

Категорія:	Національні центри обміну інформацією - взаємодіє безпосередньо з власниками/операторами
Загальний опис:	NICC є одним з 2 національних інфраструктурних центріи призначених Міністром внутрішньої безпеки відповідно до Директиви PPD-21, і слугує координаційним центром для партнерів з критичної інфраструктури для отримання ситуаційної обізнаності та інтегрованої, практичної інформації, яка може бути використана для захисту фізичних аспектів критичної інфраструктури.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	Слугує точкою входу для приватного сектору в програми безпеки та стійкості, які очолює та координує Управління захисту інфраструктури (IP) Директорату національного захисту та програм Міністерства національної безпеки США (DHS). Для отримання додаткової інформації про те, як приватний сектор співпрацює з IP, будь ласка, відвідайте https://www.dhs.gov/topic/critical-infrastructure-security. • Виконує функції адміністратора спільноти критичної інфраструктури в Інформаційній мережі національної безпеки - Критична інфраструктура (HSIN-CI), довіреної мережі для місій внутрішньої безпеки з обміну чутливою, але незасекреченою інформацією (SBU). HSIN-CI є основною системою, за допомогою якої власники та оператори приватного сектору, DHS та інші федеральні, державні та місцеві органи влади співпрацюють для захисту критичної інфраструктури країни. Для отримання додатковоїінформації про HSIN-CI, будь ласка, відвідайте https://www.dhs.gov/hsin-ci. • Обробляє та публікує звіти про підозрілу активність (SAR). Для отримання додаткової інформації про ініціативу SAR, будь ласка, відвідайте http://www.dhs.gov/how-do-i/report-suspicious-activity. • Проводить телеконференції із зацікавленими сторонами критично важливої інфраструктуричерез IP.
Звертайтеся до NICC, щоб:	Отримувати, подавати та обговорювати своєчасну, дієву та точну інформацію щодо KI • Підтримувати прямий, надійний канал зв'язку з DHS та іншими перевіреними зацікавленими сторонами сектору • Передавати інформацію про загрози, вразливості, безпеку та заходи з реагування і відновлення, що впливають на секторні та міжсекторні операції
Як зв'язатися:	:- Повідомляйте про інциденти фізичної інфраструктури або запитуйте інформацію електронною поштою NICC@hq.dhs.gov або за телефоном (202) 282-9201 • Запросіть доступ до HSIN-CI, надіславши електронного листа на адресу hsinci@hq.dhs.gov ззазначенням ◦ Ім'я та прізвище ◦ Назва ◦ Роботодавець ◦ Дійсна адреса електронної пошти ◦ Коротке письмове обґрунтування доступу, включаючи сектор(и) критичноїінфраструктури або місію, яку ви підтримуєте • Уповноважений орган розгляне вашу заявку на членство, щоб визначити, чи підходите ви для вступу. Якщо ваша заявка буде схвалена, вам буде надіслано електронного листа з інструкціями про те, як увійти в систему HSIN вперше.
У травні 2015 року NICC в **дії:**	У травні 2015 року NICC надіслав до HSIN-CI серію об'єднаних розвідувальних бюлетенів, звітів про аналіз на місцях, терористичних звітів Міністерства внутрішніх справ та інших повідомлень і документів з оцінкою ситуації щодо підвищеної загрози і необхідності бути пильними після терористичного інциденту в Гарленді, штат Техас. Ці повідомлення включали аудіозапис телеконференції зацікавлених сторін з питань критичної інфраструктури, яка надала уряду, власникам і операторам об'єктів інфраструктури форум для обміну інформацією про інциденти та загрози. IP очолює координацію та проведення телеконференцій для зацікавлених сторін у сфері критичноїінфраструктури.

Управління розвідки та аналізу (DHS I & A)	
Категорія:	Національні центри обміну інформацією - взаємодіє безпосередньо з власниками/операторами
Загальний опис:	Розвідувально-аналітичний відділ DHS США є членом IC і відіграє допоміжну роль узахисті критично важливої інфраструктури нашої держави та обміні відповідною захищеною інформацією. За допомогою свого персоналу на місцях, включаючи регіональних директорів, офіцерів розвідки, офіцерів звітності та аналітиків розвідки, управління збирає, аналізує та поширює інформацію про загрози, що стосуються критично важливої інфраструктури, на підтримку місії національної безпеки Департаменту.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	I&A використовує свою розвідку та інформацію для обміну знаннями та досвідом: • Збирає, аналізує та поширює розвідувальні дані та інформацію про загрози для критичної інфраструктури • Надає продукти та проводити брифінги щодо загроз у координації з ДРП, які мають відношення до загроз для критично важливої інфраструктури • Надає підтримку в реагуванні на інциденти іншим ключовим службам реагування DHS
Зв'яжіться з місцевим персоналомз питань внутрішнього аудиту та аудиту за адресою:	• Координуйте розвіддані та обмін інформацією про загрози, пов'язані з критичною інфраструктурою • Вимагайте проведення брифінгу щодо загроз у зв'язку з УРП
Як зв'язатися:	Напишіть на Field_Operations@hq.dhs.gov, щоб отримати інформацію про те, як зв'язатися з найближчим представником I&A.
I&A в дії:	Будь ласка, ознайомтеся з прикладами використання в розділі 4.

Консультативна рада з питань безпеки за кордоном (OSAC)

Категорія:	Партнерства, альянси та ради - Міжгалузеві - Міжнародні
Загальний опис:	OSAC був створений для сприяння відкритому діалогу між урядом США та американським приватним сектором з питань безпеки за кордоном. Сьогодні понад 4 000 організацій приватного сектору США покладаються на OSAC для отримання своєчасної та неупередженої інформації з питань безпеки та захисту. OSAC ділиться інформацією через мережу організацій-учасниць, серед яких комерційні компанії, неурядові організації (NGOs) та релігійні організації; наукові установи; 14 000 зареєстрованих користувачів веб-сайту; та149 країнових рад по всьому світу.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	Численні продукти доступні на OSAC.gov, інформаційному порталі OSAC для громадськості: • **Всі консульські повідомлення**, включаючи повідомлення з питань безпеки, поради щодо подорожей тощо. • **Звіти про злочинність та безпеку**, що надають базову інформацію про безпекове середовище в регіоні • **Інформаційні бюлетені**, що надають виборцям своєчасну інформацію про новини та події, пов'язані з безпекою • **Аналітичні звіти OSAC**, тематичні, спеціальні звіти на теми, пов'язані з безпекою • **Бібліотека ресурсів, що** включає добірку довідкових матеріалів, пов'язаних з глобальною безпекою • **Навчання**, включаючи восьмимодульну програму підвищення обізнаності про безпеку OSAC також надає кілька механізмів для обміну інформацією між представниками приватного сектору США, включаючи віртуальну підтримку, та залучення їх до співпраці. Ці зусилля включають цільові списки розсилки, орієнтовані на безпеку, та особисті зустрічі в рамках національних рад при посольствах і консульствах США. Співробітники OSAC також керують кількома регіональними радами та галузевими робочими групами. Відповідно до політики Державного департаменту США щодо відсутності подвійних стандартів (7 FAM 052),[55] OSAC координує повідомлення про конкретні, достовірні загрози смерті, серйозних тілесних ушкоджень або викрадення, які спрямовані на визначені організації приватного сектору США, що підлягають попередженню. У випадках, коли інформація про загрозу має неконкретний характер, OSAC співпрацює з Бюро консульських справ, щоб оприлюднити консульські повідомлення для попередження широкої американської спільноти.
Зв'язатися з OSAC:	- Стати організацією-засновницею • Консультуйтеся з фахівцями з регіональної безпеки OSAC щодо міжнародних загроз, з якими стикаються організації приватного сектору США • Підпишіться на сповіщення, інформаційні бюлетені та аналітичні звіти OSAC
Як долучитися:	- Соціальні мережі: @OSACState на Twitter.com • Загальна інформація: ◦ https://www.osac.gov ◦ Надішліть OSAC електронного листа на сторінку "Контакти": https://www.osac.gov/Pages/ContactUs.aspx ◦ Телефон: 571-345-2223 • Черговий офіцер (тільки в надзвичайних ситуаціях): ◦ Телефон: 202-309-5056 ◦ Електронна пошта: osac_risc@state.gov
OSAC в дії:	У 2015 фінансовому році глобальні координатори з питань безпеки OSAC виявили понад 113 конкретних і достовірних загроз для Організації приватного сектору США, що працюють по всьому світу. Сповіщення про загрози в рамках програми "Обов'язок попередити" надходили до штаб-квартир кожної організації та закордонних представництв через регіональні відділи безпеки Бюро дипломатичної безпеки при посольствах і консульствах США. Ці повідомлення координувалися з партнерами з розвідувальних і правоохоронних органів США, щоб забезпечити точність і корисність наданої інформації для пом'якшення потенційних загроз.

[55] "При адмініструванні Програми консульської інформації Державний департамент застосовує політику "не подвійних стандартів" до важливої інформації про загрози безпеці, в тому числі кримінальної інформації. Як правило, якщо Державний департамент ділиться інформацією з офіційною спільнотою США, він також повинен надавати таку ж або подібну інформацію неофіційній спільноті США, якщо загроза стосується як офіційних, так і неофіційних громадян/резидентів США" (7 FAM 052.1).

Власники та оператори Операційних центрів	
Категорія:	Власники та оператори Операційних центрів
Загальний опис:	Операційні центри власника та оператора управляються окремими суб'єктами критичної інфраструктури і, як правило, зосереджені на моніторингу та захисті активів цих суб'єктів. Однак, через різний характер потреб у безпеці кожного суб'єкта, операції та функції значно відрізняються між суб'єктами.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	• Отримання та обмін інформацією про загрози як всередині компанії, так і з ISAC та сусідніми комунальними службами • Керування всіма аспектами: ◦ Контроль доступу ◦ Системи безпеки ◦ Управління в надзвичайних ситуаціях ◦ Безперервність бізнесу завдяки використанню режиму Mission Mode ◦ Екстрені сповіщення • Реагування на інциденти
Як приєднатися:	- Суб'єкти обміну інформацією можуть зв'язатися з окремими власниками та операторами • Зовнішні власники та оператори, як правило, не пов'язані з цими центрами, за винятком можливих сусідських відносин
Оперативні та спостережні центри приватного сектору в дії:	Дивіться приклад використання електричної підстанції Metcalf у розділі 4.2 на сторінці 50.

Програма "Радник з питань захисту та безпеки" (PSA)

Категорія:	Суб'єкти, відповідальні за програми, політику та пом'якшення наслідків у сфері безпеки та стійкості критичної інфраструктури (див. Додаток С)
Загальний опис:	Управління захисту інфраструктури (IP), що входить до складу Директорату національного захисту та програм (NPPD) Міністерства національної безпеки США, керує Програмою PSA. PSA - це експерти з питань безпеки, які співпрацюють з партнерами урядової місії SLTT і членами спільноти зацікавлених сторін з приватного сектору для захисту критично важливої інфраструктури країни. Програма PSA підтримує потужний оперативний потенціал на місцях, а Головне управління з питань безпеки та PSA обслуговує всі 50 штатів і території США. Регіональні представництва та підрозділи PSA слугують сполучною ланкою між ресурсами захисту інфраструктури DHS; координують оцінку вразливості, навчання та інші продукти і послуги DHS; забезпечують життєво важливий зв'язок для обміну інформацією в стаціонарному режимі та при реагуванні на інциденти; а також допомагають власникам і операторам об'єктів в отриманні допуску до об'єктів безпеки.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	PSA має 5 напрямків діяльності, які безпосередньо підтримують захист критично важливої інфраструктури: • Планування, координація та проведення обстежень і оцінок безпеки - PSAs проводять добровільні, нерегулярні обстеження та оцінки безпеки об'єктів критичної інфраструктури у своїх регіонах. • Планування та проведення інформаційно-просвітницьких заходів - PSAs проводять інформаційно-просвітницькі заходи з власниками та операторами об'єктів критичної інфраструктури, громадськими групами та релігійними організаціями на підтримку пріоритетів у сфері IP • Підтримка національних заходів з питань спеціальної безпеки (NSSE) та заходів Рейтингу активності спеціальних подій (SEAR) - УРП надають підтримку федеральним, державним та місцевим посадовцям, відповідальним за планування, керівництво та координацію заходів NSSE та SEAR. • Реагування на інциденти - PSAs планують і, за вказівкою, розгортають Об'єднані територіальні командні групи, Об'єднані оперативні центри, Регіональні координаційніцентри реагування Федерального агентства з надзвичайних ситуацій та/або Державні та місцеві центри з надзвичайних ситуацій у відповідь на природні або техногенні інциденти. • Координація та підтримка тренінгів з підвищення обізнаності про саморобні вибухові пристрої та зменшення ризиків - PSAs співпрацюють з Управлінням із запобігання вибухам IP, координуючи тренінги та надаючи матеріали партнерам з SLTT, щоб допомогти їм у стримуванні, виявленні, запобіганні, захисті та реагуванні на загрози, пов'язані з саморобними вибуховими пристроями.
Зверніться до найближчого PSA, щоб:	• Отримувати, надавати та обговорювати своєчасну, дієву та точну інформацію щодо критичної інфраструктури • Підтримувати прямий, надійний канал зв'язку з DHS та іншими перевіреними зацікавленими сторонами сектору • Передавати інформацію про загрози, вразливості, безпеку та заходи з реагування та відновлення, що впливають на секторні та міжсекторні операції • Дізнатися більше про ресурси захисту критичної інфраструктури, включаючи тренінги на такі теми, як активні стрільці, саморобні вибухові пристрої та внутрішні загрози: https://www.dhs.gov/critical-infrastructure-training
Як долучитися:	Для отримання додаткової інформації або для того, щоб зв'язатися з найближчим PSA, будь ласка, звертайтеся заадресою: PSCDOperations@hq.dhs.gov.
Програма PSA в дії:	Починаючи з 2005 року, PSA залучає партнерів урядових місій та представників приватного сектору до захисту критично важливої інфраструктури країни. Станом на 2016 рік вони провели сотні оцінок вразливості та оглядів безпеки. PSA підтримали інформаційно-просвітницьку кампанію "Допомога у забезпеченні безпеки під час масових заходів", а також численні спеціальні заходи, зокрема, Суперкубок 50 і новорічну ніч на Таймс-Сквер. PSA надавали допомогу в ліквідації наслідків стихійних лих (повені, зимові шторми) і координували численні тренінги, в тому числі презентації програми "Активний стрілець", а також курси з виявлення об'єктів спостереження і семінари з інформування про саморобні вибухові пристрої та управління загрозою вибуху, організовані Управлінням із запобігання вибухам.

Секторні координаційні ради (SCCs)

Категорія:	Партнерства, альянси та ради - галузеві
Загальний опис:	Галузеві координаційні ради (SCCs) - це самоорганізовані, самокеровані та самоврядні ради, що складаються з власників та операторів, їхніх галузевих асоціацій, постачальників та інших осіб, які взаємодіють з широкого кола галузевих стратегій, політик, заходів та питань. SCCs слугують основними пунктами співпраці між урядом, власниками та операторами в питаннях безпеки та стійкості критичної інфраструктури. Вони є аналогом Урядових координаційних рад (GCCs) у приватному секторі.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	SCCs координують та співпрацюють з організаціями в рамках усієї партнерської структури NIPP, включаючи галузеві агентства (SSAs), відповідні GCCs, Міжгалузеву раду з питань критичної інфраструктури, Координаційну раду з питань державного, місцевого, племінного та територіального управління (SLTTGCC), Регіональну координаційну раду консорціуму (RC3) та Федеральну раду вищого керівництва, для вирішення всього спектру питань безпеки та стійкості критичної інфраструктури для кожного сектору. SCCs слугують голосом сектору і є основними точками входу для уряду, щоб співпрацювати з сектором у сфері безпеки та стійкості критичної інфраструктури. Інші основні функції SCCs можуть включати в себе: • Слугує стратегічним механізмом комунікації та координації між власниками, операторами, галузевими асоціаціями, постачальниками та урядом під час виникнення загроз або операцій з реагування та відновлення, як це визначеногалуззю. • Визначення, впровадження та підтримка відповідних можливостей та механізмів обміну інформацією в секторах, де не існує жодної структури обміну інформацією • Заохочення членства у репрезентативному секторі • Участь у плануванні, пов'язаному з циклічним переглядом Національного плану захисту інфраструктури (NIPP), розробкою та переглядом галузевих планів (SSP), а також щорічним поданням галузевих заходів до DHS • Сприяння зусиллям, спрямованим на забезпечення інклюзивної організації та координацію розробки політики сектору щодо планування та забезпечення безпеки і стійкості критичної інфраструктури, навчань і тренувань, інформування громадськості, а також пов'язаних з цим заходів і вимог щодо впровадження. • Виявлення, розробка та обмін інформацією в секторі (як державного, так і приватного сектору) щодо ефективних практик кібербезпеки, таких як робочі групи з кібербезпеки, оцінки ризиків, стратегії та плани. • Надання інформації уряду щодо зусиль та потреб сектору у сфері досліджень і розробок
Зверніться до SCC для:	Отримання інформації про дії промисловості та уряду щодо пріоритетів захисту критичної інфраструктури для вирішення галузевих та міжгалузевих проблем.
Як долучитися:	На веб-сайті DHS надається додаткова інформація про кожен з 16 секторів критичної інфраструктури, включаючи статути SCC та членство в них: https://www.dhs.gov/scc
SCC в дії:	див. приклад використання Havex/BlackEnergy в Розділі 4.1 на стор. 45 та приклад використання підстанції Metcalf в Розділі 4.2 на стор. 50.
Веб-сайти SCC:	- Хімічний (CSCC): www.chemicalcybersecurity.org • Комерційні об'єкти: https://www.dhs.gov/commercial-facilities-sector-council-charters-and-членство • Комунікації (CSCC): www.commscc.org • Критичне виробництво (CMSCC): https://www.dhs.gov/critical-manufacturing-sector-council- charters-membership • Дамби (DSCC): https://www.dhs.gov/dams-sector-council-charters-and-membership • Оборонно-промислова база (DIBSSC): https://www.dhs.gov/defense-industrial-base- sector-council-charters-and-membership • Служби з надзвичайних ситуацій (ESSCC): www.sheriffs.org/content/emergency-service-sector- coordinating-council-esscc

Секторні координаційні ради (SCC)

- Енергія
  - Підсектор електроенергетики (ESCC): http://www.electricitysubsector.org/
  - Нафтогазовий підсектор (ONGSCC): https://www.dhs.gov/energy-ong-subsector-charters-and-membership
- Фінансові послуги (FSSCC): www.fsscc.org
- Харчування та сільське господарство (FASCC): https://www.dhs.gov/food-and-agriculture-sector-council-charters-and-membership
- Державні установи (GFSCC): https://www.dhs.gov/government-facilities-sector-council-charter-membership
- Охорона здоров'я та громадське здоров'я (HSCC): www.phe.gov/cip
- Інформаційні технології (ITSCC): www.it-scc.org
- Ядерні реактори, матеріали та відходи (NRMWSCC): https://www.dhs.gov/nuclear-sector-council-charters-and-membership
- Транспорт (TSCC): https://www.dhs.gov/transportation-sector-charters-and-membership
- Системи водопостачання та водовідведення (WSCC): https://www.dhs.gov/water-sector-council-charters- and-membership

Галузеві агентства (SSA)

Категорія:	Суб'єкти, відповідальні за програми, політику та пом'якшення наслідків у сфері безпеки та стійкості критичної інфраструктури (див. Додаток С)
Загальний опис:	Президентська політична директива 21 (PDD-21) "*Безпека та стійкість критичної інфраструктури*" сприяє об'єднанню національних зусиль для зміцнення та підтримки безпечної, функціонуючої та стійкої критичної інфраструктури. Кожен сектор критичної інфраструктури має унікальні характеристики, операційні моделі та профілі ризиків. Як наслідок, PDD-21 призначає для кожного сектору галузеве агентство (SSA) або спів- агентства SSA, які володіють інституційними знаннями та спеціалізованим досвідом у своєму секторі (секторах). У секторах, що підлягають федеральному або державному регулюванню, SSA співпрацює з відповідним регулятором. SSA сприяють обміну інформацією між секторами та підтримують національну програму, вирішуючи спільні національні пріоритети та звітуючи про прогрес у досягненні результатів у сфері безпеки тастійкості.
Ролі та обов'язки SSA щодо власників/операторів об'єктів критичної інфраструктури та приватного сектору:	Кожна SSA використовує свої особливі знання та досвід, щоб: • Координувати та співпрацювати з DHS та іншими відповідними федеральними міністерствами та відомствами, з власниками та операторами об'єктів критичної інфраструктури, з незалежними регуляторними органами (за необхідності), а також з організаціями SLTT, за необхідності, з метою виконання PDD-21. • Слугувати щоденним федеральним інтерфейсом для динамічного визначення пріоритетів, співпраці та координації галузевої діяльності • Виконувати обов'язки з управління інцидентами відповідно до встановлених законом повноважень та інших відповідних політик, директив чи положень • Надавати, підтримувати або сприяти наданню технічної допомоги та консультацій для цього сектору з метою виявлення вразливостей та пом'якшення наслідків інцидентів, за необхідності • Підтримувати встановлені законом вимоги міністра внутрішньої безпеки щодо звітності, надаючи на щорічній основі інформацію про критичну інфраструктуру в конкретних секторах.
Зверніться до свого SSA:	Кожен SSA має свої особливості, але вам слід зв'язатися з кожним SSA (контактна інформація на наступних сторінках), щоб дізнатися, чи можуть вони вам допомогти: • Координувати та співпрацювати з галузевими урядовими та промисловими партнерами для розробки спільних стратегій, які сприятимуть підвищенню безпеки та стійкості критичної інфраструктури • Визначити потреби та прогалини у плануванні, ініціативах, політиках та процедурах, які впливають на спроможність сектору захищати критичну інфраструктуру • Обмінюватися інформацією щодо загроз, вразливостей, безпеки та заходів з реагування і відновлення, які впливають на секторні та міжсекторні операції • Отримувати доступ до галузевих довідників, посібників та навчальних веб-курсів
Як підключитися:	- Нижче наведено список SSA та пов'язаних з ними секторів • Нижче наведено веб-сайти та контактну інформацію для різних SSA • Веб-сайт DHS надає більше інформації про кожен з 16 секторів критичної інфраструктури, включаючи Плани для конкретних секторів: https://www.dhs.gov/sector-specific-agencies
SSA в дії:	DHS, як SSA для комерційних об'єктів, спонсорує Форум з питань секретної розвідки для приватного сектору (CIF). В рамках DHS, Управління розвідки та аналізу (I&A) і Управління національного захисту та програм (NPPD) двічі на місяць проводять зустрічі в штаб- квартирі DHS з представниками критичної інфраструктури приватного сектору, які мають відповідний допуск, в рамках Сектору комерційних об'єктів і Міжсекторальної координаційної ради (CSCC). CIF було розширено на регіональному рівні для отримання зворотного зв'язку від представників приватного сектору. Цей зворотний зв'язок може допомогти в розробці поточних і майбутніх розвідувальних продуктів та інших відповідних ініціатив з обміну інформацією або аналітичних ініціатив.

Комерційні об'єкти
Дамби критично важливих для комунікацій виробничих об'єктів
Інформаційні технології екстрених

Галузеві агентства (SSAs)		
Сектори SSAs та критичної інфраструктури	Відомство, що відповідає за конкретний сектор	Сектор критичної інфраструктури
	Міністерство сільського господарства (USDA) Управління з харчових продуктів та медикаментів (FDA)	Харчування та сільське господарство
Джерело: PDD-21, Безпека та стійкість критичної інфраструктури 12.02.2013: https://www.whitehouse.gov/t he-pressoffice/2013/02/12/presidential -policy-directive-criticalinfrastructure-security-andresil, а також Додаток B до NIPP 2013 (стор. 43): http://www.dhs.gov/publicatio n/nipp-2013-partneringcritical-infrastructure-securityand-resilience	Міністерство оборони (DOD)	Оборонно-промислова база
	Міністерство енергетики (DOE)	Енергетика
	Департамент охорони здоров'я та соціальних служб (HHS)	Охорона здоров'я та громадське здоров'я
	Управління казначейства	Фінансові послуги
	Агентство з охорони навколишнього середовища (EPA)	Послуги водопостачання та водовідведення
	Департамент внутрішньої безпеки (DHS)	Хімічна промисловість Комерційні об'єкти Комунікації Критичне виробництво Дамби Аварійні служби Інформаційні технології Ядерні реактори, матеріали та відходи
	Департамент внутрішньої безпеки Адміністрація загального обслуговування (GSA)	Державні установи
	Департамент внутрішньої безпеки Департамент транспорту (DOT)	Транспортні системи

Контактні особи SSA:[60]

Сектор	Агенція/організація	Офіс/Центр	Електронна пошта	Веб-сайт
Хімічна промисловість	DHS	Управління захисту інфраструктури	chemicalsector@hq.dhs.gov	www.dhs.gov/chemical-sector
Критичне виробництво			criticalmanufacturing@hq.dhs.gov	www.dhs.gov/critical-виробничий сектор
Комерційні об'єкти			cfsteam@hq.dhs.gov	www.dhs.gov/commercial-facilities-sector
Дамби			dams@hq.dhs.gov	www.dhs.gov/dams-sector
Служби екстреної допомоги			ESSTeam@hq.dhs.gov	www.dhs.gov/emergency-services-sector

[56] Департамент сільського господарства відповідає за сільське господарство та продукти харчування (м'ясо, птиця та перероблені яєчні продукти).

[57] Управління з контролю за продуктами харчування та лікарськими засобами відповідає за продукти харчування, крім м'яса, птиці та перероблених яєчних продуктів.

[58] Енергетичний сектор включає виробництво, переробку, зберігання, передачу та розподіл нафти, газу та електроенергії, в той час як Міністерство внутрішньої безпеки є органом, відповідальним за комерційні об'єкти атомної енергетики та дамби.

[59] Департамент освіти є головним розпорядником коштів для підсектору "Об'єкти освіти" Сектору державних об'єктів; Департамент внутрішніх справ є головним розпорядником коштів для підсектору "Національні пам'ятники та ікони"Сектору державних об'єктів.

[60] Вибрано з "Функціональних взаємозв'язків безпеки та стійкості критично важливої інфраструктури" - DHS, червень 2013 року;оновлено у квітні 2016 року.

Сектор	Агенція/організація	Офіс/Центр	Електронна пошта	Веб-сайт
Ядерні реактори, матеріали та відходи			NuclearSSA@hq.dhs.gov	www.dhs.gov/nuclear-reactors-materials-and-waste-sector
Комунікації		Управління кібербезпеки та зв'язку(CS&C)	Comms_Sector@hq.dhs.gov	www.dhs.gov/office-cybersecurity-and-communications
Інформаційні технології			-	www.dhs.gov/office-cybersecurity-and-communications
Транспортні системи		Адміністрація транспортної безпеки (TSA)	TransportSector@tsa.dhs.gov	http://www.dhs.gov/transportation-systems-sector
		Берегова охорона США - Управління з контролю за дотриманням вимог у портах та на об'єктах	-	www.uscg.mil/hq/cg5/cg544
	DOT	Офіс Секретаря	-	www.transportation.gov/mission/administrations/intelligence-security-emergency-response/security-policy-plans-division
Державні установи	DHS	Федеральна служба охорони	NIPP-GFS@hq.dhs.gov	www.dhs.gov/government-facilities-sector
	GSA		-	
Оборонно-промислова база	DOD	Помічник міністра оборони з питань внутрішньої оборони та безпеки в Америці	RSS.DCIPOffice@osd.mil	http://policy.defense.gov/OUSDPOffices/ASDforHomelandDefenseGlobalSecurity/DefenceCriticalInfrastructureProgram/Roles.aspx
Енергія	DOE	Дирекція з постачання електроенергії та енергонадійності - Відділ безпеки інфраструктури та відновлення енергопостачання	doehqeoc@oem.doe.gov	http://energy.gov/oe/mission/infrastructure-security-and-energy-restoration-restoration-iser
Фінансові послуги	Treasury	Управління захисту критичної інфраструктури та комплаєнс-політики	OCIP@treasury.gov	www.treasury.gov/about/organizational-structure/offices/Pages/--Office of-Critical-Information-Protection-and-Compliance-Policy.aspx -Office of-Critical-Information- Protection-and-Compliance- Policy.aspx
Продовольство та сільське господарство	USDA	Управління внутрішньої безпеки та координації надзвичайних ситуацій	nsps@dm.udsa.gov	www.dm.usda.gov/ohsec/hsd/fas.html
	FDA	Управління продовольчого захисту, комунікації та реагування на надзвичайні ситуації	fooddefense@fda.hhs.gov	www.fda.gov/Food/FoodDefense/default.htm
Охорона здоров'я та громадське здоров'я	HHS	Офіс помічника Секретаря з питань готовності та реагування	cip@hhs.gov	www.phe.gov/Preparedness/planning/cip/Pages/default.aspx
Системи водопостачаннята водовідведення	EPA	Відділ водної безпеки	-	www.epa.gov/waterresilience

Берегова охорона США (USCG) - Районні комітети морської безпеки (AMSC) і Хвилі на набережній (WOW)	
Категорія:	Партнерства, альянси та ради - галузеві
Загальний опис:	**Регіональні комітети з морської безпеки (AMSC)** - це державно-приватні партнерства по всій країні, які координують свою діяльність з USCG для вирішення місцевих питань, пов'язаних з безпекою та захистом порту або водного шляху. До складу комітетів, як правило, входять місцеві представники державних органів, морських профспілок і галузевих організацій, а також громадських організацій. AMSC існують у кожній зоні капітана порту (COTP) і є наріжним каменем безпеки в портахкраїни. **Хвилі на набережній (WOW)** - це періодичне видання, що виходить раз на два місяці, розроблене Управлінням відповідності портів та об'єктів Берегової охорони, щоб тримати зацікавлених осіб в курсі проблем безпеки, охорони та управління.
Функції, продукти та послуги, що мають відношення до спільноти критичної інфраструктури:	**AMSC:** • Служити сполучною ланкою між зацікавленими сторонами порту для інформування про загрози та зміни в рівнях морської безпеки та розповсюдження відповідної інформації про безпеку • Визначення критично важливої портової інфраструктури та операцій • Визначте ризики, загрози, вразливості та наслідки • Визначте стратегії пом'якшення наслідків та методи їх реалізації • Розробити та описати процес постійної оцінки загальної безпеки порту шляхом аналізу наслідків та вразливостей, як вони можуть змінюватися з часом, і які додаткові стратегії пом'якшення наслідків можуть бути застосовані • Надання консультацій та допомоги COTP у розробці Плану безпеки на морі (AMSP) • Забезпечити, щоб оцінка морської безпеки на основі оцінки ризиків була виконана самим AMSC, місцевим COTP, групою з оцінки портової безпеки берегової охорониабо третьою стороною. **WOW:** • Випускає щомісячний інформаційний бюлетень
Зверніться до AMSC або WOW, щоб:	• Отримати більше інформації про AMSCs • Додати до списку розсилки WOW • Подати статтю на розгляд у WOW
Як зв'язатися:	- Веб-сайт AMSC з посиланням на брошуру: http://www.uscg.mil/hq/cg5/cg544/amsc.asp • Електронна пошта AMSC: AMSC@uscg.mil • WOW та AMSC POC: CG-FAC@uscg.mil
AMSC в дії:	Інформація про загрози, що надходить через COTP від USCG в кожному конкретному випадкучерез AMSC.
WOW в дії:	Останні випуски можна знайти за посиланням: http://www.uscg.mil/hq/cg5/cg544/Waves%20on%20the%20Waterfront.asp

Варіанти використання

Наступні приклади використання ілюструють, як відбувався обмін інформацією про загрози в чотирьох реальних ситуаціях, пов'язаних з різними загрозами:

1. Кібер: Havex та BlackEnergy (2014)
2. Фізичний: Інцидент з Меткалфом (2013)
3. Міжнародний: Напад на торговий центр Westgate в Кенії (2013)
4. Національна подія спеціального характеру: Інавгурація Президента України 2013 року

На додаток до графіків у кожному варіанті використання, див. Додаток G для більш детальної візуалізації інформаційних потоків у кожному з варіантів використання.

4.1 Приклад використання кіберпростору: Havex та BlackEnergy (2014)

Цей приклад ілюструє взаємодію між приватними компаніями з кібербезпеки, компаніями з промислового контролю та федеральними органами, що займаються інформаційно-просвітницькою діяльністю та залученням зацікавлених сторін, у відповідь на дві кіберзагрози. Зауважте, що це не є вичерпним поясненням всього обміну інформацією, пов'язаного з цією справою. Джерела інформації були обмежені відповідями на інформаційні запити.

4.1.1 Передумови

У цьому прикладі використання кіберпростору розглядається пара загроз для промислових систем управління (ICS), які були вперше виявлені в середині 2014 року, але виникли ще на початку 2011 року. Про першу, під назвою Havex, Національному центру інтеграції кібербезпеки і зв'язку (NCCIC) повідомили приватні фірми, що займаються кібербезпекою. Друге шкідливе програмне забезпечення, під назвою BlackEnergy, було виявлено довіреними сторонніми партнерами. Оскільки обидві кіберзагрози мали аспекти, спрямовані на системи ICS критичної інфраструктури США, Група реагування на кібернетичні надзвичайні ситуації в ICS (ICS-CERT), яка є частиною NCCIC, взяла на себе провідну роль у проведенні скоординованої інформаційно-роз'яснювальної роботи, пом'якшенні наслідків та реагуванні від імені федерального уряду.

Шкідливе програмне забезпечення Havex використовувалося для різних цілей, але в кампанії був варіант, орієнтований на ICS, який використовував кілька векторів для зараження. Серед них були фішингові електронні листи, перенаправлення на інші веб-сторінки та інфіковані інсталятори програмного забезпечення ICS. Найуспішнішим вектором зараження були інсталятори програмного забезпечення на веб-сайтах постачальників ICS. Коли оператори ICS, нічого не підозрюючи, завантажували оновлену версію програмного забезпечення ICS, вони також мимоволі встановлювали шкідливе програмне забезпечення Havex на свої комп'ютери. На основі звітів дослідників двох приватних постачальників систем комп'ютерної безпеки та подальшого аналізу, проведеного NCCIC, шкідливе програмне забезпечення продемонструвало можливості сканування та контролю доступу до середовища системи контролю доступу, в тому числі потенційно маніпулюючи цим процесом. Зловмисник Havex продемонстрував знайомство зі специфічною технологією систем управління (протокол Open Platform Communications або OPC) і зміг використати цю можливість для сканування та опитування скомпрометованої мережі на предмет наявності пристроїв системи управління. Розвитокцієї можливості також вказує на те, що зловмисник провів певний рівень досліджень і тестування для розробки шкідливого програмного забезпечення Havex.

Шкідливе програмне забезпечення BlackEnergy використовувало раніше невідомі вразливості в людино-машинному інтерфейсі (HMI), за допомогою якого оператор контролює та керує системою управління, щонайменше трьох продуктів постачальників ICS. Маючи доступ до HMI, зловмисник може робити все, що може робити законний оператор, наприклад, вмикати та вимикати обладнання, бачити стан процесу та змінювати задані значення системи, включаючи допустимий рівень резервуару або максимальну температуру. Глибина цих потенційних втручань у систему управління становить серйозну загрозу для стабільності процесу і створює потенціал для фізичних наслідків. Аналіз методів, які використовував суб'єкт загрози BlackEnergy, виявив цілеспрямовані зусилля, спрямовані на пошук і використання раніше невідомих вразливостей у пристроях і програмному забезпеченні систем управління. Ці зусилля вимагали спеціальних досліджень пристроїв і програмного забезпечення систем управління, а також тестування для отримання можливості проведення успішної атаки.

Ці дві кампанії ілюструють узгоджені зусилля, які протягом щонайменше чотирьох років докладали висококваліфіковані зловмисники, щоб зрозуміти системи управління критичною інфраструктурою, виявити невідомі/невиправлені вразливості для експлуатації та використати "нестандартні" методи для отримання доступу до операційного середовища. Хоча повний масштаб проникнення в системи ICS залишається невідомим, скоординована інформаційно-просвітницька кампанія, розпочата федеральним урядом у відповідь на ці загрози, поінформувала і навчила багато компаній і організацій, а також потенційно вплинула на осіб, які несуть відповідальність за ICS.

4.1.2 Обмін інформацією про загрози

4.1.2.1 DHS - NCCIC

NCCIC і його компонент ICS-CERT працювали спільно з FBI над виявленням потенційних суб'єктів загрози і виконанням традиційних заходів реагування на інциденти. Було підготовлено та розповсюджено каналами "Для службового користування" (FOUO) глибокий 47-сторінковий аналітичний звіт щодо Havex та BlackEnergy, а також двосторінкове резюме для керівників. NCCIC також проводив інші заходи з обміну інформацією про загрози:

- Координували роботу з постраждалими постачальниками для виявлення вразливостей у програмному забезпеченні та їх виправлення
- Розробили власний алгоритм виявлення та розповсюдили його на загальнодоступному сайті
- Випустили серію попереджень рівня "Не для друку/для службового користування" (U//FOUO) для спільноти критичної інфраструктури через портал ICS, портал Інформаційної мережі національної безпеки (HSIN) та публічний веб-сайт ICS-CERT, а також співпрацювали з розвідкою та правоохоронними органами з метою обмеження обсягу інформації, яка може бути використана супротивниками.
- Проведення "Кампанії дій", що складалася з "секретних" брифінгів у 13 містах для понад 1700 допущених зацікавлених сторін і координувала інформаційно-роз'яснювальну роботу в рамках Кампанії через Центри обміну інформацією та аналізу (ISACs); галузеві агентства (SSAs); партнерів на рівні штатів, місцевих, племінних і територіальних громад (SLTT); радників з питань захисту інфраструктури (PIP) Офісу захисту інфраструктури (PSAs) Міністерства безпеки США; об'єднані центри; і FBI.
- Проведення захищених відеоконференцій рівня "Секретно" (SVTC) з об'єднаними центрами та польовими офісами FBI
- Проводив брифінги на всіх звичайних інформаційних заходах ICS-CERT (щотижневих, щомісячних, щоквартальних, спеціальних) з грифами "Несекретно" та "Таємно"
- Співпрацювали з розвідувальним співтовариством (IC), щоб краще зрозуміти та описати загрозу

4.1.2.2 Multi-State ISAC (M S-ISAC)

Багатодержавний ISAC (MS-ISAC) допоміг обмінюватися інформацією, поширивши презентацію ICS-CERT про кібер-ризики для промислових систем управління під назвою "BlackEnergy & Havex Briefing for Partners" у квітні 2015 року. MS-ISAC також розгорнув сигнатури для виявлення Havex і Black Energy в Альберті,[61] але це не дало жодного підтвердженого збігу.

4.1.2.3 Міністерство енергетики США (DOE)

Міністерство оборони США отримало розвідувальні повідомлення про випадки BlackEnergy та Havex від приватних постачальників послуг з кібербезпеки. DOE провело ручну перевірку і змогло переконатися, що жодна з компаній не була включена до списків постачальників або ICS-CERT. Міністерство енергетики працювало з ISAC над тим, щоб поділитися незасекреченою інформацією та інформацією з відкритих джерел з членами організації. Вони звернулися до ISAC з проханням поділитися інформацією зі своїми членами у вигляді запиту на інформацію (RFI). В результаті власники та оператори змогли поділитися з МНКБ будь-якою інформацією, що стосувалася справ BlackEnergy/Havex, яку вони мали. Члени ISAC з допуском і клієнти з обмеженим допуском були особисто проінструктовані в офісах Міністерства енергетики США і отримали інформацію до рівня "Цілком таємно/Делікатна інформація з обмеженим доступом" (TS/SCI). DHS провело регіональну кампанію Havex/BlackEnergy, а DOE заохочувало власників/операторів брати участь у регіональних зустрічах, на яких ділилися інформацією з грифом "Таємно".

4.1.2.4 DHS - IP

За необхідності (як у випадках з компаніями Havex та BlackEnergy) HIC посилює свою інформаційно-пропагандистську діяльність, скликаючи робочі групи для обговорення конкретної загрози або проблеми, які об'єднують потенційно постраждалих партнерів з приватного сектору та представників федерального уряду. Ці робочі групи створюються для посилення типової ролі HIC у сприянні співпраці та координації між урядом і приватним сектором у рамках процесу Консультативної ради з питань партнерства у сфері критичної інфраструктури (CIPAC).

Під час розслідувань справ Havex та BlackEnergy робоча група з нерозсекреченої спеціальної тематики звернулася до керівників Секторальної координаційної ради (СКР), профільних експертів та інших представників високого рівня з проханням скликати нараду для обміну інформацією про загрози.
Близько 30 представників приватного сектору взяли участь особисто, а деякі з них - через конференц-зв'язок. Під час зустрічі ICS-CERT провів брифінг щодо загрози BlackEnergy/Havex, включаючи інформацію про передумови виникнення загрози та стратегії пом'якшення її наслідків. На основі консенсусних порад та рекомендацій учасників зустрічі ICS-CERT підготував односторінкову брошуру про BlackEnergy/Havex, призначену для вищого керівництва, в якій узагальнено інформацію про загрозу та потенційні наслідки, і яку було розповсюджено серед IB, зокрема, серед них

[61] Albert - це служба моніторингу та аналізу мережевого потоку/систем виявлення вторгнень MS-ISAC, яка надає своїм партнерам автоматизований процес, що працює майже в режимі реального часу, який виявляє та сповіщає про традиційні та сучасні загрози в мережі, сприяючи швидкому реагуванню на загрози та атаки. Датчики Albert забезпечують традиційний моніторинг системи виявлення вторгнень (IDS), а також збір та аналіз мережевого потоку і пасивного DNS. Через цілодобовий Операційний центр безпеки (SOC) MS-ISAC керує датчиками для виявлення зловмисної активності та, відповідно до процедур ескалації, визначених партнером, надає повідомлення про зловмиснуактивність.

розміщєна в Інформаційній мережі національної безпеки (HSIN)[62]. Крім того, була створенаі розміщена вкладка BlackEnergy/Havex на сайті HSIN, щоб забезпечити "живий" доступ до інформації про BlackEnergy/Havex.

4.1.2.5 DHS - Управління розвідки та аналізу (I&A)

У червні 2015 року компанія I&A у співпраці з ICS-CERT опублікувала Звіт про польовий аналіз (FAR) - готовий продукт розвідувального аналізу "(U//FOUO) Нещодавні кампанії зловмисного програмного забезпечення підкреслюють загрозу для промислових систем управління в регіоні Скелястих гір", в якому було проаналізовано, як кампанії зловмисного програмного забезпечення Havex і BlackEnergy вплинули на критично важливу інфраструктуру в регіоні Скелястих гір. Цей аналіз ґрунтувався на доказах і дослідженнях, зібраних ICS-CERT, а також на технічних звітах з відкритих джерел від постачальників антивірусних програм. Продукт був опублікований і поширений відділом внутрішнього аудиту та його співробітниками на місцях за допомогою різних засобів, включаючи брифінги про загрози, Спільноту інтересів HSIN-Intel, інформаційні електронні листи, вручення ключовим клієнтам і заплановані телефонні дзвінки. Звіт був поширений і використаний в першу чергу федеральними партнерами, SLTT і партнерами з приватного сектору - в тому числі державними і великими міськими об'єднаними центрами - з метою допомогти в оцінці ризиків і розгортанні ресурсів для їхнього зменшення. Виконком також опублікував низку розвідувально-інформаційних звітів (IIR), які детально описують кампанії шкідливого програмного забезпечення BlackEnergy проти державних, місцевих та приватних об'єктів в Огайо, Північній Каролiні, Массачусетсі, Каліфорнії, Джорджії та Алабамі. Ці звіти були надані в розпорядження ІС і отримали позитивні відгуки від багатьох партнерів з громадськості.

4.1.2.6 DHS - Адміністрація транспортної безпеки (TSA)

Управління транспортної безпеки, як одне з галузевих агентств (SSA), співпрацювало з ICS-CERT для забезпечення присутності зацікавлених сторін на регіональних брифінгах під грифом "Таємно". Управління розвідки та аналізу (OIA) також включило факти використання кейсу до різних оцінок "Секретно" та "Несекретної/чутливої інформації з питань безпеки (U/SSI)", які були передані наступним зацікавленим сторонам за допомогою наступних механізмів:

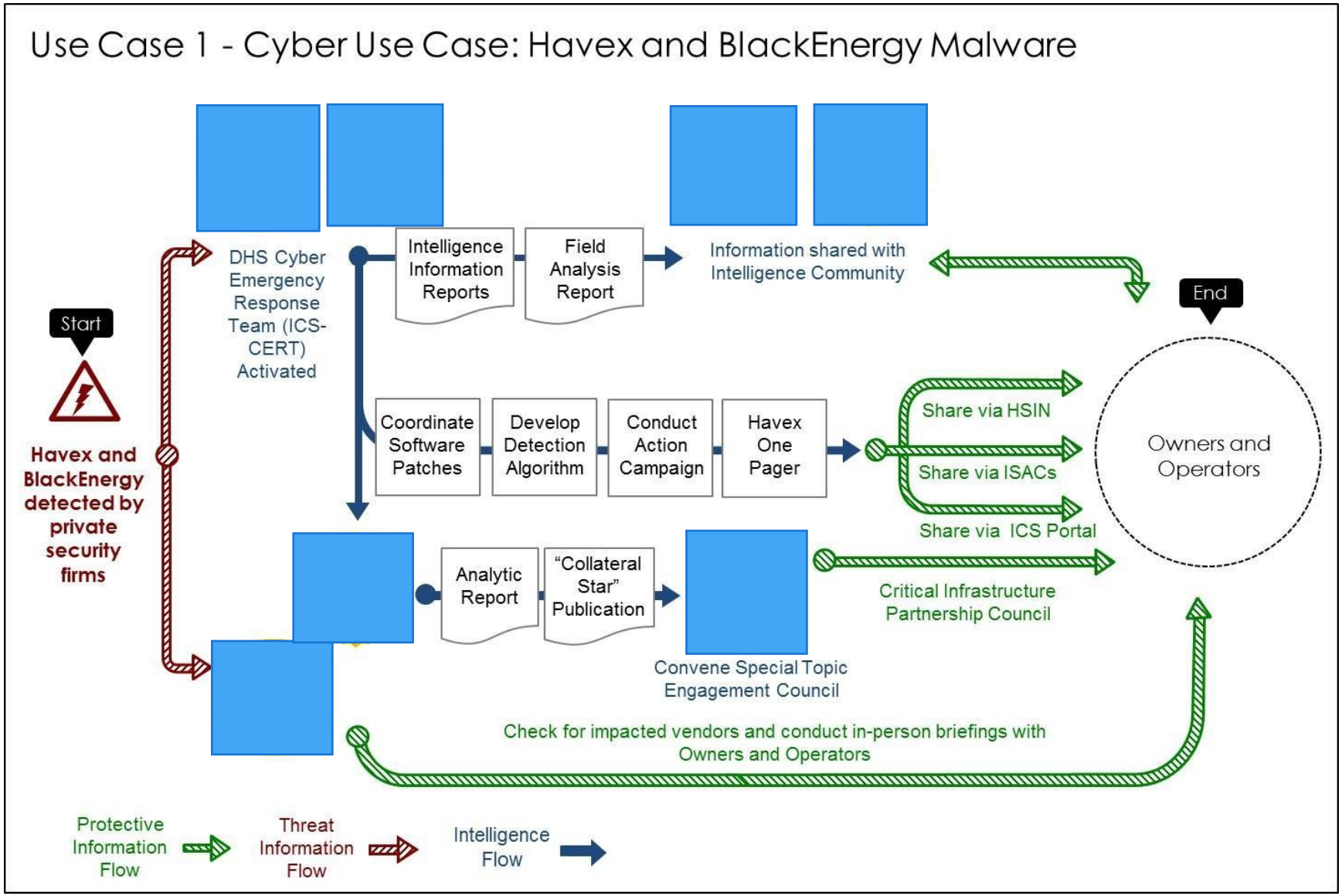
- Засекречені анклави "Секретно":
  - Електронна пошта (партнери Уряду США)
  - Особисті зустрічі (з Урядом США та приватним сектором)
  - Безпечні відео-телеконференції (SVTC) (Уряд США та приватний сектор)
  - Безпечна телеконференція (Уряд США та приватний сектор)
  - Об'єднані світові системи розвідувального зв'язку (JWICS) (включно з Національним антитерористичним центром (NCTC) онлайн) (партнери USG)
  - Національна мережа захищених даних (HSDN) (включаючи NCTC Online) (партнери USG)
  - Віддалений доступ Адміністрації транспортної безпеки до секретних відеоматеріалів (TRACE MOVI) (Уряд США та приватний сектор)
  - Засекречені дискусії та/або читання засекречених матеріалів для тих, хто не перебуває в столичному регіоні, через офіцерів польової розвідки TSA
- Некласифіковані (включаючи FOUO та SSI) як для Уряду США, так і для партнерів з приватного сектору:

[62] HSIN - це надійна мережа для операторів та партнерів місій з національної безпеки, яка дозволяє обмінюватися чутливою, але нерозкритою інформацією. Федеральні органи, SLTT, міжнародні та приватні партнери з національноїбезпеки використовують HSIN для управління операціями, аналізу даних, надсилання попереджень та повідомлень, і загалом для обміну інформацією, необхідною для виконання своєї роботи.

- Електронна пошта
- Особисто
- Телеконференція
- HSIN

У цьому та всіх інших випадках, коли FBI публікує Спільну оцінку загроз (JTA) або Міністерство внутрішніх справ надсилає Спільний розвідувальний бюлетень, Звіт про польовий аналіз або Звіт про тероризм Міністерства внутрішніх справ, TSA`s OIA надсилає інформацію до своєї мережі офіцерів польової розвідки (FIOs). Якщо інформація є засекреченою, Відділ інтеграції розвідувальних даних (IIB) Відділу польової розвідки переглядає і передає інформацію у версії TRACE MOVI з грифом "Таємно" офіцерам польової розвідки. До цієї інформації регулярно додаються інструкції щодо її розповсюдження, в тому числі серед федеральних партнерів або приватних зацікавлених сторін. Нарешті, деякі матеріали також зводяться в щоденний секретний підсумковий звіт, який називається "Щоденний польовий інформаційний звіт" (DFIR)[63] для розповсюдженняна місцях.

[63] Раніше DFIR називався Звітом про обізнаність щодо стратегічних транспортних загроз (STTAR).



Малюнок 9: Варіант використання 1 - Кібернетичний варіант використання: шкідливе програмне забезпечення Havex та BlackEnergy

4.2 Фізичний приклад використання: Інцидент на електричній підстанції в Меткалфі (2013)

Цей практичний приклад ілюструє обмін інформацією про загрози, який відбувся після фізичного нападу на електропідстанцію, що включав розрив оптоволоконних кабелів. У прикладі також обговорюються різні методи інформування на національному рівні, які застосовувалися протягом року після інциденту. Зауважте, що це не є вичерпним поясненням всього обміну інформацією, пов'язаного з цим випадком. Джерела інформації були обмежені відповідями на інформаційні запити.

4.2.1 Передумови

16 квітня 2013 року нападники випустили понад 100 пострілів у радіатори охолодження 17 електричних трансформаторів на електричній підстанції компанії Pacific Gas and Electric (PG&E) в Меткалфі, штат Каліфорнія. Внаслідок обстрілу з радіаторів витекло тисячі галонів охолоджувальної рідини. Сигналізація про падіння тиску змусила персонал PG&E вимкнути трансформатори, щоб запобігти незворотнім пошкодженням. Незважаючи на радіаторну атаку, PG&E змогла успішно перенаправити електроенергію, щоб уникнути будь-яких втрат електроенергії для клієнтів. Однак, окрім того, що зловмисники обстріляли радіатори трансформаторів, вони також розірвали дві групи оптоволоконних кабелів на прилеглій до підстанції території. Перерізання цих кабелів призвело до переривання стаціонарного телефонного зв'язку, в тому числі служби 911, в частині округу Санта-Клара, Каліфорнія. Подвійна атака тривала близько години і завдала збитків на мільйони доларів. Особа (особи), відповідальна (відповідальні) за атаку, не встановлена.

4.2.2 Обмін інформацією про загрози

4.2.2.1 ГІГІЄНА ТА БЕЗПЕКА

Після нападу PG&E негайно зв'язалася з місцевими правоохоронними органами та посилила безпеку, забезпечивши цілодобову присутність на підстанції Metcalf та інших важливих підстанціях, додавши додаткові пости охорони за підтримки правоохоронців округу Санта-Клара. Офіс шерифа округу Санта-Клара очолив розслідування спільно з поліцією Сан-Хосе. Розслідування також розпочало місцеве відділення FBI у Сан-Франциско.

Після звернення до місцевих правоохоронних органів PG&E негайно подала Звіт про аварійну ситуацію в електромережі (форма OE-417) до Управління постачання електроенергії та енергетичної надійності (OE) Міністерства енергетики США (DOE), а також Звіт про підозрілу діяльність (SAR) до Управління захисту інфраструктури (IP) Міністерства внутрішньої безпеки США (DHS). Це ініціювало поширення інформації про інцидент серед інших федеральних партнерів.

Після атаки PG&E звернулася до державних і приватних партнерів з проханням поділитися інформацією про інциденти та загрози за допомогою наступних кроків:

- В режимі телеконференції представник Координаційної ради сектору гребель PG&E (SCC)[64] обговорив ситуацію з головою SCC з питань гребель.
- Після цього дзвінка PG&E проінформувала Спільну раду сектору дамб, що складається з КРГС та Координаційної ради уряду з питань гребель (GCC).

[64] PG&E також є членом КРК дамб.

- PG&E також проінформувала Координаційну раду електроенергетичного підсектору (ESCC) під час наради, яку Рада скликала для забезпечення обізнаності щодо ситуації, обміну інформацією та координації дій членів. ІВ скоординував з ESCC участь представників Федеральної комісії з регулювання енергетики (FERC), Федеральної комісії зв'язку (FCC), Міністерства енергетики (DOE), FBI та Регіонального розвідувального центру Північної Каліфорнії (NCRIC) у цій нараді.
- PG&E також провела брифінг в Інституті електротехніки Едісона (EEI), щоб забезпечити обізнаність щодо ситуації та поділитися відповідною інформацією.

По мірі надходження нової інформації директор з безпеки PG&E продовжував ділитися нею з партнерами та проводив оновлені брифінги для SCCs, EEI та Міністерства енергетики (DOE). Інші постачальники енергії з приватного сектору отримували інформацію через звіти SAR та веб-портали Інформаційної мережі національної безпеки - критична інфраструктура (HSIN-CI) та HSIN-Dams.

На додаток до обміну інформацією, PG&E надала радникам з питань захисної безпеки (PSAs) компанії IP в Каліфорнії доступ до своїх основних підстанцій для проведення обстежень безпеки, які допомогли зменшити загрозу. Після інциденту місцеві PSA надають постійну допомогу PG&E в оцінці вразливості системи безпеки, розробці варіантів захисних заходів та плануванні безпеки. В результаті нападу багато власників/операторів енергосистеми також провели огляд своїх критично важливих активів і поточних заходів безпеки. Згодом вони розробили плани для усунення прогалин івразливостей та вжили додаткових заходів, щоб бути готовими до подібних атак у майбутньому. Наприклад, на основі події в Меткалфі компанія Dominion (постачає електроенергію до Вірджинії та Північної Кароліни) розробила семирічний план посилення безпеки вартістю 500 мільйонів доларів, відомий як "Програма надійності та безпеки Dominion".

4.2.2.2 Департамент енергетики (DOE)

Як галузеве агентство (SSA) для енергетичного сектору, Міністерство енергетики провело інформаційно-координаційну нараду з представниками Міністерства безпеки, Федеральної комісії з регулювання енергетики, Федеральної комісії зв'язку, FBI та Національної комісії з регулювання радіочастот США (NCRIC).

4.2.2.3 DHS - IP

IP також організував окрему телефонну розмову з FERC, FCC, FBI та NCRIC для ознайомлення з ситуацією. За первинними заходами послідувала взаємодія із зацікавленими сторонами державного та приватного секторів в енергетичному секторі, в ході якої зацікавлені сторони обговорили актуальність інциденту, а зусилля з обміну інформацією були поширені на суміжні сектори критичної інфраструктури, такі як сектор дамб. Всі відповідні Ситуаційні звіти (SARs) були передані через Національний інфраструктурний координаційний центр (NICC) відповідним зацікавленим сторонам критичної інфраструктури в енергетичному секторі та PSAs.

4.2.2.4 НКРЗІ,НКРЕ та ЕС -ISAC

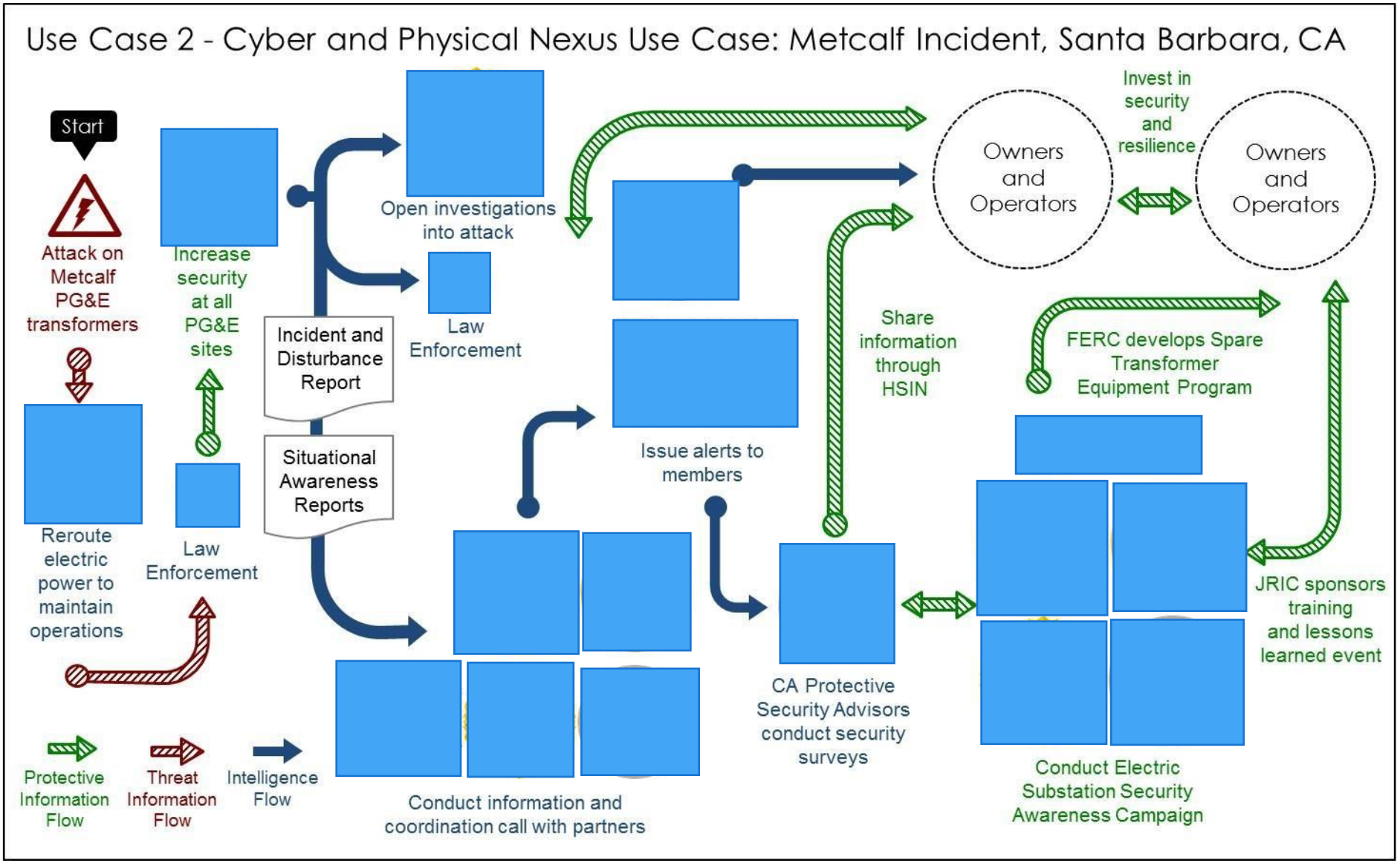
NCRIC, Північноамериканська корпорація з надійності електропостачання (NERC) та Сектор енергетики ISAC (ES-ISAC) розіслали попередження своїм партнерам у секторі, включаючи власників та операторів об'єктів критичної інфраструктури, не згадуючи конкретно про PG&E.

4.2.2.5 Каліфорнійський об'єднаний регіональний розвідувальний центр (JRIC)

Через три місяці після атаки обмін інформацією переріс у спільні навчання. 23 липня 2013 року Каліфорнійський об'єднаний регіональний розвідувальний центр (JRIC) організував навчальний захід для обговорення інциденту та обміну досвідом. Серед доповідачів були представники PG&E Security та іншої каліфорнійської енергетичної компанії. На брифінгу також були присутні представники PSAs в Каліфорнії.

4.2.2.6 Спільна ініціатива

Крім того, у відповідь на інцидент з "Меткалфом", DHS та Міністерство енергетики (DOE), у координації з міжвідомчими партнерами та приватним сектором, розпочали інформаційно-просвітницьку кампанію з підвищення рівня обізнаності з питань безпеки в електроенергетиці. Кампанія з підвищення обізнаності щодо безпеки електричних підстанцій розпочалася в грудні 2013 року і завершилася в березні 2014 року. Вона була проведена у співпраці з ESCC, ES-ISAC, FBI, FERC та численними галузевими партнерами, включаючи PG&E. Це "роуд-шоу" відбулося в 10 містах США та 3 містах Канади. Кожен захід включав серію брифінгів, а також панельну дискусію для підвищення обізнаності про мінливе середовище ризиків та сприяння розширенню співпраці щодо стратегій зменшення ризиків, захисних заходів та найкращих галузевих практик. Спочатку сесії були відкриті для зацікавлених сторін зі спільноти власників і операторів електроенергії та правоохоронних органів, але згодом до них долучилися представники служб з надзвичайних ситуацій, нафтогазового та ядерного секторів.



Малюнок 10: Варіант використання 2 - Кібер-фізичний взаємозв'язок: Інцидент у Меткалфі, Санта-Барбара, Каліфорнія

4.3 Міжнародний приклад використання: Атака на Вестгейт-Молл у Найробі, Кенія (2013)

Атака на торговий центр Вестгейт-Молл у Найробі, Кенія, у 2013 році викликала великий інтерес у приватному секторі США, оскільки вона продемонструвала вразливість моделі відкритого доступу, яка використовується у більшості комерційних об'єктів, у тому числі в американських торгових центрах. Тактика, методи і процедури, що використовувалися, були важливими для розуміння зацікавленими сторонами, щоб керувати підготовкою. Цей приклад ілюструє інформаційно-роз'яснювальну роботу та взаємодію федерального уряду з партнерами з сектору комерційних об'єктів після нападу на торговельний центр Вестгейт-Молл. Зауважте, що це не вичерпне пояснення всього обміну інформацією, пов'язаного з цим випадком. Джерела інформації були обмежені відповідями на інформаційні запити.

4.3.1 Передумови

21 вересня 2013 року четверо нападників, озброєних пістолетами і гранатами, увірвалися до торгового центру Вестгейт-Молл в Найробі, Кенія. Нападники вчинили штурм, який завершився чотириденним протистоянням з кенійськими силами безпеки. Сомалійське угруповання "Аль-Шабааб" взяло на себе відповідальність за напад, що зробило його найбільшою атакою угруповання після двох скоординованих вибухів смертників в Уганді, які забрали життя 70 осіб у 2010 році. Угруповання стверджувало, що напад на Вестгейт-Молл мав на меті помститися кенійському уряду за його участь у сомалійському конфлікті.

Загалом, в результаті зіткнення загинула щонайменше 71 людина (в тому числі шестеро співробітників служби безпеки і всі четверо нападників) і понад 175 отримали поранення. Крім того, кенійський уряд заявив, що врятував понад 1000 осіб. Ряд американських компаній володіють вітринами у Вестгейт-Моллі, і під час нападу в торговому центрі працювали співробітники кількох американських компаній. Тимчасовий співробітник корпорації "Болл" отримав вогнепальне поранення під час інциденту і згодом був евакуйований назад до США.

4.3.2 Обмін інформацією про загрози

4.3.2.1 Консультативна рада з питань безпеки за кордоном Державного департаменту США (OSAC)

Консультативна рада з питань безпеки за кордоном при Державному департаменті США (OSAC), яка сприяє відкритому діалогу з питань безпеки між урядом США і американським приватним сектором за кордоном, зробила свій внесок у початкову реакцію уряду США на атаку на Вестгейт-Молл, координуючи як короткостроковий, так і довгостроковий обмін інформацією та заходи реагування, пов'язані з цим інцидентом. Країнова рада OSAC в Найробі швидко почала обмінюватися інформацією про атаку, використовуючи веб-додатки для розміщення записів камер відеоспостереження, наданих одним із членів OSAC з приватного сектору, а також для надання оновленої інформації з місця подій. Ця інформація дозволила офіцеру регіональної безпеки Державного департаменту США з питань дипломатичної безпеки координувати подальші дії з відповідним юридичним аташе FBI, а також з іншими федеральними відомствами, які брали участь у реагуванні.
Регіональний аналітик OSAC у Східній Африці також прилетів до Найробі наступного тижня після нападу, щоб очолити засідання Країнової ради. Після участі OSAC у телефонній конференції, організованій Міністерством внутрішніх справ США з приводу цього інциденту, понад 50 членів OSAC (включаючи комерційні об'єкти та власників і операторів транспорту) звернулися до OSAC з проханням проконсультуватися з регіональними аналітиками.

Загалом, регіональні аналітики OSAC надають індивідуальні консультації на спеціальній основі із зареєстрованими представниками виборчих округів для надання експертних порад з питань

безпеки або аналізу щодо низки регіональних проблем, які викликають занепокоєння. Консультації можуть бути найрізноманітнішими: деякі призначені для надання загальної ситуаційної обізнаності про певне середовище, тоді як інші більше зосереджені наконкретній проблемі безпеки.

4.3.2.2 ISAC з нерухомості (RE-ISAC)

Отримавши повідомлення про атаку, Центр обміну та аналізу інформації про нерухомість (RE-ISAC) почав спілкуватися зі своїми членами щодо інциденту. Через день після інциденту він надав членам коротке резюме, а також розповсюдив його серед партнерів удержавному секторі для ознайомлення, в тому числі в Управлінні захисту інфраструктури (IP) Міністерства національної безпеки (в тому числі радників з питань безпеки IP); Управлінні розвідки і аналізу (PSAs) Міністерства національної безпеки; Раді Альянсу внутрішньої безпеки (DSAC); OSAC; FBI; і об'єднаних центрах. Вона надавала оновлення через щоденні звіти, в яких використовувалися дослідницькі платформи з відкритим вихідним кодом, постачальники розвідувальних даних (за різними підписками), а також урядові оновлення і аналітичні дані (в тому числі інформація, якою ділилися DHS і OSAC).
Протягом наступних днів RE-ISAC продовжував ділитися останніми даними від OSAC зі своїми членами, в тому числі надавав оновлену інформацію про деякі з каскадних впливів інциденту на вітчизняні об'єкти. Протягом наступних тижнів керівництво RE-ISAC надавало оновлену інформацію телефоном та електронною поштою міжгалузевій спільноті (наприклад, під час засідання Національної ради ISAC у жовтні 2013 року), колегам у секторах та підсекторах (коли члени групи розпочали підготовку до сезону святкових покупок), а також партнерам з федерального уряду на всіх рівнях (насамперед FBI та DHS), об'єднаним центрам та правоохоронним органам, оскільки члени групи працювали з урядом над проведенням навчань з підготовки до святкових сезонів.

RE-ISAC та його члени продовжують уважно стежити за подіями і були дуже заангажовані,коли Аль-Шабааб опублікував відеозаписи з погрозами західним торговим центрам у лютому 2015 року. Тоді RE-ISAC допоміг поінформувати про загрозу членів, партнерів та інші галузеві ISAC.

4.3.2.3 Федеральне бюро розслідувань (FBI)

Після першого нападу на Вестгейт місцеві відділення FBI провели брифінги про загрози для партнерів Об'єднаної антитерористичної групи (JTTF), включаючи виконавчі ради JTTF, військові робочі групи, власників і операторів приватного сектору, організації, що забезпечують безпеку торгових центрів, і співробітників правоохоронних органів.
Інформація, надана на цих брифінгах, варіювалася від останніх новин до перших результатів розслідування та інших форм необроблених розвідувальних даних (з відповідним рівнем секретності для кожної аудиторії). FBI також ділилося інформацією про загрози електронною поштою і через портал InfraGard, а багато місцевих відділень FBI проводили відеоконференції для обговорення уроків, винесених з Вестгейту.

FBI також співпрацювало з Міністерством національної безпеки та іншими партнерами, щоб забезпечити більш інтенсивні та довгострокові зусилля з підготовки та навчання власників і операторів американських торговельних центрів і роздрібних торговців найкращим практикам, пов'язаним з комплексними атаками. Після інциденту FBI попросило Відділ інформаційно-просвітницької роботи та програм (SOPD) DHS-IP швидко налагодити зв'язки з ключовими представниками галузі, а SOPD, у свою чергу, зв'язався з Координаційною радою сектору комерційних об'єктів (SCC), щоб залучити ключових лідерів до Ради підсектору торгових центрів. Потім ці лідери розповіли про важливість цієї ініціативи своїм мережам і заохотили їх до активної участі. Разом FBI та IP сприяли проведенню 56 обговорень у відділеннях FBI по всій країні з 6 по 9 грудня 2013 року.
У навчаннях взяли участь державні, місцеві, приватні та федеральні партнери (включно зIP`s PSAs). Місцеві відділення FBI також провели 61 командно-штабне навчання, 57 командно-штабних навчань і 53 повномасштабні навчання для перевірки планів і процедур готовності до сценарію, схожого на напад на Вестгейт. Загалом у них взялиучасть 9 472 особи.

4.3.2.4 Спільний комітет з оцінки заходів боротьби з тероризмом (JCAT)

Спільна група JCAT, що складається з фахівців з реагування на *надзвичайні ситуації на* федеральному рівні та рівні штатів (на чолі з Національним контртерористичним центром (NCTC), за участю представників FBI та Міністерства внутрішніх справ), 20 грудня 2013 року підготувала "*Комплексні операційні умови для фахівців з реагування на надзвичайні ситуації - торгові центри",* щоб допомогти в реагуванні на надзвичайні ситуації в торговельних центрах. Цей продукт був також переданий приватному сектору через InfraGard і DSAC, а також розміщений на порталі правоохоронних органів FBI (LEEP) і в Інформаційній мережі національної безпеки (HSIN).

4.3.2.5 DHS - Федеральне агентство з надзвичайних ситуацій (FEMA)

Навчання та семінари, організовані NCTC, FBI та FEMA, тривають з часу теракту в Мумбаї 2008 року. Наприклад, Спільна серія семінарів з підвищення обізнаності щодо боротьби з тероризмом (Joint Counterterrorism Awareness Workshop Series, JCTAWS) - це дводенні семінари для міст першого рівня (найбільших міст США), покликані покращити здатність місцевих органів влади готуватися до складних терористичних атак, захищатися від них і реагувати на них. У 2012 році FEMA розширило своє портфоліо комплексних атак, включивши до нього чотириденний Інтегрований курс з управління в надзвичайних ситуаціях (IEMC) "Підготовка громад до комплексної скоординованої атаки", який зосереджується на містах другого і третього рівнів. Як і семінар, курс є навчальною ініціативою, спрямованою на посилення спроможності місцевих органів влади захищатися від комплексних скоординованих атак і реагувати на них. Обидві програми включають брифінги (в тому числі брифінг про загрози від Національного антитерористичного центру), тематичні дослідження та фасилітовані дискусії на основі сценарію нападу, характерного для конкретної громади.[65] Під час таких обговорень учасники самостійно визначають прогалини у своїх поточних оперативних планах і можливостях, а також шукають можливі рішення.

Після нападів на торговельний центр Вестгейт-Молл багато громад звернулися з проханням включити торговельний центр до сценаріїв JCTAWS та IEMC. В результаті, ці громади провели активні дискусії про те, як розпочати інтегроване, скоординоване реагування на активний напад стрільця або комплексний напад на їхні торгові центри таключові об'єкти роздрібної торгівлі. У семінарах взяли участь керівники служб безпеки торговельних центрів, і в результаті дискусій були чітко сформульовані прогалини в плануванні, координації та оперативних можливостях, над усуненням яких ці спільноти зараз працюють над подальшим розвитком.

4.3.2.6 DHS - IP

З часу нападу на Вестгейт-Молл підхід до тренувань змінився у відповідь на зміни в середовищі загроз. У другій половині 2014 року в літературі насильницького екстремізму з'явилося багато закликів до нападів на федеральні та військові об'єкти, комерційні об'єкти, а також до нападів з використанням вогнепальної та іншої холодної зброї. У жовтні 2014 року IP скликав Робочу групу з питань взаємодії (EWG), до складу якої увійшли представники роздрібної торгівлі, готельного бізнесу, уряду та інші, щоб обговорити ситуацію із загрозами та подальші кроки. В результаті IP, Міжвідомчий комітет з безпеки (ISC),[66] та NCTC розпочали Ініціативу з підвищення рівня безпеки, кампанію в 11 містах, яка включала брифінги про загрози та дискусії на відкритих форумах. Ініціатива об'єднала федеральних і комерційних партнерів, а також служби екстреного реагування на ключових ринках країни.

[65] Партнери з приватного сектору, які беруть участь у роботі JCTAWS та IEMC, зазвичай включають телекомунікаційних/мережевих провайдерів; комунальні служби; великих роботодавців - страхові, фінансові, виробничі, хімічні, логістичні та туристичні компанії; готелі; місця проведення спеціальних заходів; представників ділових кіл/палат уцентрі міста; неприбуткові організації - Американський Червоний Хрест, Волонтерські організації, що діють в умовах надзвичайних ситуацій (VOAD), або релігійні мережі. З 2010 року було проведено 20 семінарів JCTAWS, в яких взялиучасть понад 4 500 осіб.

[66] Мандат ISC полягає у підвищенні якості та ефективності фізичної безпеки та захисту будівель і невійськових федеральних об'єктів у Сполучених Штатах.

Після того, як у лютому 2015 року "Аль-Шабааб" опублікував відеоролик із закликом до подальших нападів, зокрема, з посиланням на "Молл оф Америка", PSAs завершив хвилю оцінок інфраструктури торговельних центрів за допомогою Інструменту обстеження інфраструктури (IST).[67] У березні 2015 року IP скликав аналогічну EWG з партнерами з приватного сектору, щоб обговорити, як модифікувати серію семінарів з підготовки до активних дій проти стрільців, що проводяться Міністерством внутрішніх справ США, щоб впровадити більше методів навчання для дорослих і дозволити більш динамічний обмін інформацією з аудиторією. Нарешті, нещодавно IP скликав ще одну групу, подібну до EWG - цього разу за участю Міністерства оборони - після нападу на центри рекрутингу і резерву в Чаттанузі, штат Теннессі, що стався 16 липня 2015 року і призвів до загибелі чотирьох морських піхотинців і одного офіцера TN США. Такі робочі групи вивчають нові загрози і обговорюють нові підходи до запобігання, захисту і реагування на потенційні атаки.

4.3.2.7 DHS - Управління розвідки та аналізу (I&A)

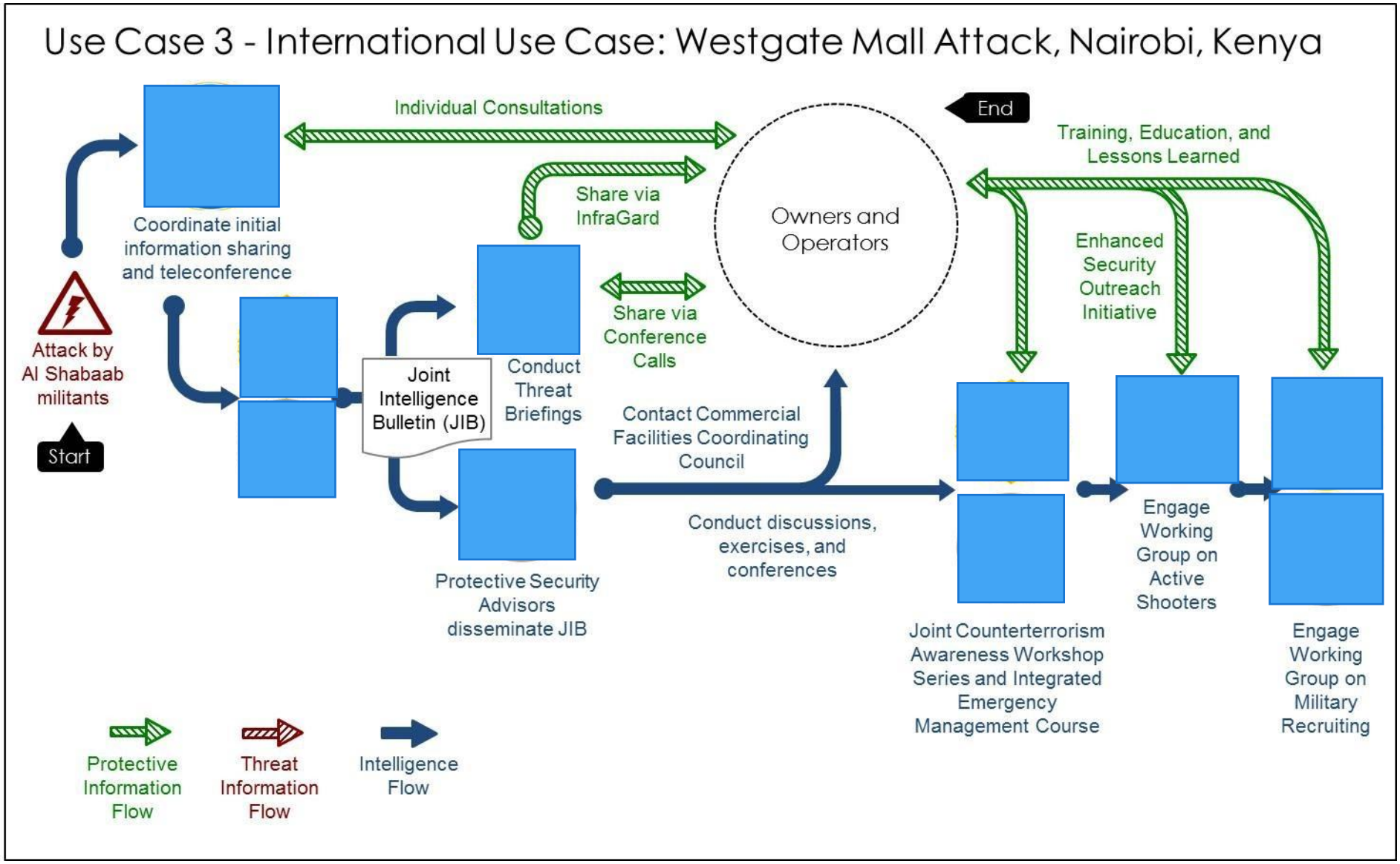
Крім того, через свій Відділ польових операцій I&A координував брифінги про загрози для торговельних центрів по всій країні. В штаті Огайо співробітник відділу розвідки (IO) у координації з місцевим PSA провів брифінг щодо загроз і взяв участь у круглому столі з питаннями та відповідями в місцевому об'єднавчому центрі - Центрі стратегічного аналізу та інформації (SAIC). Понад 40 менеджерів з безпеки з місцевих торгових центрів відвідали брифінг на організованій SAIC нараді з питань безпеки місцевих торгових центрів у Департаменті громадської безпеки штату Огайо. Крім того, офіцер з питань безпеки провів засекречений брифінг щодо загроз під час щомісячного брифінгу DHS-SAIC з обміну розвідданими та інформацією про загрози. Офіс в Огайо також співпрацював з SAIC над публікацією оцінки загроз "Тільки для службового користування" (FOUO), призначеної для служб швидкого реагування, правоохоронних органів, пожежників тощо, і розміщеної на сайті HSIN-Intel та в Системі управління контактною інформацією штату Огайо (CIMS).

У торговому центрі Вестгейт-Молл у штаті Кентуккі офіційний представник поінформував про загрозу місцевих посадовців під час зустрічі, організованої місцевим органом державної охорони здоров'я. IO також проінформував інших партнерів на державному, місцевому, племінному та територіальному рівнях (SLTT), особливо тих, хто може відреагувати або співпрацювати з операторами торговельного центру в подібному випадку.

На початку 2015 року I&A та FBI випустили Спільний розвідувальний бюлетень (JIB) щодо чергової загрози для торговельних центрів наприкінці січня - на початку лютого. Спільний бюлетень був розповсюджений серед федеральних партнерів та партнерів SLTT, а також серед ключових власників, операторів та партнерів з приватного сектору. Супроводжуючи спільну аналітичну записку партнерам у зонах відповідальності (AOR), співробітники I&A у Східно-Центральному регіоні також підготували супровідну записку, або "Погляд з місця", в якій описали регіональний, державний та місцевий контекст. Місцева PSA змогла допомогти в поширенні цієї JIB та супровідної записки. Результатом цих зусиль також став звіт про підозрілу діяльність (SAR).

Крім того, співробітники Південно-Центрального регіону польових операцій I&A також провели брифінг щодо загроз для поліції Гарленда та сусідніх правоохоронних органів. Цей брифінг охоплював тактику, методи і процедури (TTPs), що використовувались під час нападу 2013 року в торговому центрі Вестгейт-Молл в Кенії, а також інших міжнародних терористичних атак.

[67] Веб-інструмент оцінки вразливості, який застосовує зважені бали для виявлення вразливостей і тенденцій для конкретної інфраструктури та всього сектору.



Малюнок 11: Приклад використання 3 - Міжнародний приклад використання: Напад на торговий центр Westgate, Найробі, Кенія

4.4 Приклад використання національної події особливої важливості (NSSE): інавгурація президента 2013 року

Цей приклад ілюструє структуру взаємодії між федеральними органами, SLTT та власниками і операторами критичної інфраструктури до і під час заздалегідь запланованої національної події спеціального призначення (NSSE), що вимагає підвищеного рівня кібер-та фізичної безпеки через велику кількість учасників. Зауважте, що це не є вичерпним поясненням всього обміну інформацією, пов'язаного з цією справою. Джерела інформації були обмежені відповідями на інформаційні запити.

4.4.1 Передумови

Секретар Департаменту внутрішньої безпеки (DHS) визначив інавгурацію президента у Вашингтоні, округ Колумбія, у січні 2013 року як NSSE (національна безпекова подія, що має національне значення). (NSSE - це подія національного або міжнародного значення, яка, на думку DHS, є потенційною мішенню для тероризму або іншої злочинної діяльності. Прикладами є саміти світових лідерів, зустрічі міжнародних організацій та з'їзди з висунення кандидатів у президенти). Надання статусу NSSE вимагає від федеральних агентств повної співпраці та підтримки для забезпечення безпеки та захисту тих, хто береучасть у заході або відвідує його, а також безпеки та захисту громади, в якій відбуваєтьсязахід.

Інавгурація 2013 року тривала з 20 по 22 січня і включала різноманітні публічні та приватні заходи, в тому числі саму церемонію, парад, що її супроводжував, обід і три офіційні інавгураційні бали. Урочистості привернули увагу понад мільйона відвідувачів до Національного столичного регіону (NCR), а понад 3 000 поліцейських і військових контингентів допомогли забезпечити необхідний рівень безпеки. Різноманітні організації обмінювалися інформацією про загрози як напередодні, так і під час заходу, допомагаючи підтримувати безпеку.

4.4.2 Діяльність з обміну інформацією про загрози на етапі, що передуєпопередженню

FBI і DHS були основними федеральними відомствами та агентствами, які ділилися інформацією про загрози з власниками/операторами критичної інфраструктури та суб'єктами приватного сектору щодо подій під час інавгурації. Як і під час усіх заходів NSSE, FBI було провідним федеральним агентством з розвідки та управління кризовими ситуаціями, DHS - Федеральне агентство з надзвичайних ситуацій (FEMA) - з ліквідації наслідків, а DHS - Секретна служба США (USSS) - з координації планування та реалізації заходів безпеки відповідно до Закону Президента США "Про захист від загроз" від 2000 року. Інші відомства та установи були залучені до інших компонентів підготовки та моніторингу безпеки в режимі реального часу.

Для інавгураційних заходів було розроблено та опубліковано Спільну оцінку загроз (JTA) з грифом "Не для друку/для службового користування" (U//FOUO). У JTA розглядалися міжнародні та внутрішні терористичні, кримінальні, кібернетичні та транспортні загрози, пов'язані з інавгурацією та NCR. Члени розвідувального співтовариства створюють JTAs, а FBI є провідною розвідувальною організацією з їх розробки. Серед інших основних учасників - Управління розвідки та аналізу (I&A) Міністерства оборони США, Штаб Об'єднаних сил і DC Fusion Center - Вашингтонський регіональний центр з аналізу загроз і аналізу загроз. Додаткову інформацію надали Адміністрація транспортної безпеки (TSA) ,Берегова охорона США (USCG), Національний контртерористичний центр (NCTC), поліція Капітолію США, Регіональний розвідувальний центр Північної Вірджинії і Центр скринінгу

тероризму. Після підготовки JTA був переданий федеральним, державним і місцевиморганам влади та управління, щоб допомогти їм розробити і визначити пріоритети захисних і допоміжних заходів. Потім він був широко розповсюджений серед власників/операторів об'єктів критичної інфраструктури NCR через HSIN, зустрічі з місцеві правоохоронні органи та об'єднані центри, а також несекретні та секретні брифінги. Інша інформація надавалася за необхідності. JTA не знайшла жодної інформації, яка б вказувала на реальну загрозу для інавгурації Президента України 2013року, але вона містила оцінку поточного загрозливого середовища.

4.4.2.1 DHS - Секретна служба США (USSS) та Управління захисту інфраструктури (IP)

Окрім розповсюдження JTA, для керівників підприємств були проведені брифінги Підкомітетом із захисту критичної інфраструктури (CIPSC), який очолював USSS та співголовою якого був представник IP. CIPSC був одним з 28 перших підкомітетів, створених Виконавчим керівним комітетом (створеним USSS). До складу CIPSC увійшли понад 100 учасників з державного та приватного секторів, включаючи власників/операторів об'єктів критичної інфраструктури, радників з питань захисту та безпеки (PSAs) IP, FBI, паркову поліцію США, окружну поліцію та Департамент транспорту округу Колумбія. Перед CIPSC було поставлено завдання розробити та впровадити план захисту критичної інфраструктури з метою моніторингу та захисту всіх інфраструктурних систем у постраждалому районі, щоб забезпечити безпечне середовище та сприяти зменшенню потенційних ризиків для громадської безпеки. CIPSC зосередився на фізичній та віртуальній критичній інфраструктурі в Північно-Кавказькому та Середньо-Атлантичному регіонах, яка була настільки важливою, що непрацездатність або руйнування цієї інфраструктури могло мати виснажливий вплив на інавгурацію Президента України. Як приклад таких брифінгів, 9 січня 2013 року CIPSC провів незасекречений брифінг для помічника секретаря з питань інтелектуальної власності Міністерства внутрішніх справ США та численних керівників комунальних підприємств, присвячений майбутнім заходам з підготовки до інавгурації.

Додатковими компонентами обміну інформацією про загрози під час інавгурації були брифінги та тренінги, які PSAs проводили для власників та операторів об'єктів критичної інфраструктури. IP спільно з USSS визначили системи та об'єкти критичної інфраструктури, які забезпечували проведення інавгураційних заходів, а також пов'язаних з ними учасників. Після цього PSAs у NCR зв'язалися з відповідними власниками/операторами об'єктів критичної інфраструктури та провели оцінку або використали попередні оцінки ключових об'єктів критичної інфраструктури та місць у NCR. Це допомогло власникам і операторам підготуватися до інавгураційних заходів і надало основним федеральним департаментам і відомствам інформацію про стан готовності ключових об'єктів критичної інфраструктури. Нижче наведено кілька прикладів використаних інструментів, оцінок і планів щодо критичної інфраструктури:

- Книги геопросторових карт
- Дослідження безпеки за допомогою інструменту Infrastructure Survey Tool (IST)
- Платформи візуалізації інфраструктури (IVP), раніше - комп'ютерний інструментоцінки (CBAT)

PSA також співпрацювала з Управлінням із запобігання вибухам (OBP) для проведення тренінгів для 275 членів уряду та приватних організацій NCR, включаючи власників/операторів об'єктів критичної інфраструктури, таких як водоканал округу Колумбія. Цей тренінг включав низку різноманітних курсів на теми, пов'язані з безпекою, такі як обізнаність про м'які цілі, виявлення саморобних вибухових пристроїв та підготовка активних стрільців.

4.4.3 Діяльність з обміну інформацією про загрози під час заходу

4.4.3.1 DHS - Секретна служба США (USSS) Міжвідомчий координаційний центр (MACC)

Під час інавгураційних заходів інформацією про загрози також обмінювався персонал, який підтримував різні федеральні, штатні та місцеві операції і командні центри. Відділ DHS-IP, розташований у Міжвідомчому координаційному центрі (MACC) під управлінням USSS, був основним координаційним центром для діяльності PSA, пов'язаної з інавгураційними заходами. Він забезпечував цілодобове покриття. Відділ DHS-IP у Координаційному центрі з питань критичної інфраструктури (CICC) USSS США слугував альтернативним координаційним центром.

Під час інавгурації в CICC перебували представники 27 компаній приватного сектору. PSAs використовували низку формальних і неформальних процесів для обміну інформацією. Вони включали особисте спілкування з представниками критичної інфраструктури, які засідали в CICC, телефонні дзвінки та електронні листи для обміну інформацією про загрози критичній інфраструктурі з власниками/операторами об'єктів критичної інфраструктури. Вони були готові координувати свої дії з USSS і FBI для обміну інформацією, якщо виникне така потреба. CICC також надавав звіти до MACC, Національного координаційного центру інфраструктури (NICC) та Оперативного управління DHS.

Служба спостереження та оповіщення NICC підтримувала свою роботу в постійному режимі 24 години на добу 7 днів на тиждень. PSAs використовували точкові звіти (SPOTREP) для обміну інформацією з NICC та операціями IP, коли це було необхідно, та надання оновленої інформації про стан інцидентів на об'єктах критично важливої інфраструктури.

4.4.3.2 DHS - Офіс розвідки та аналізу

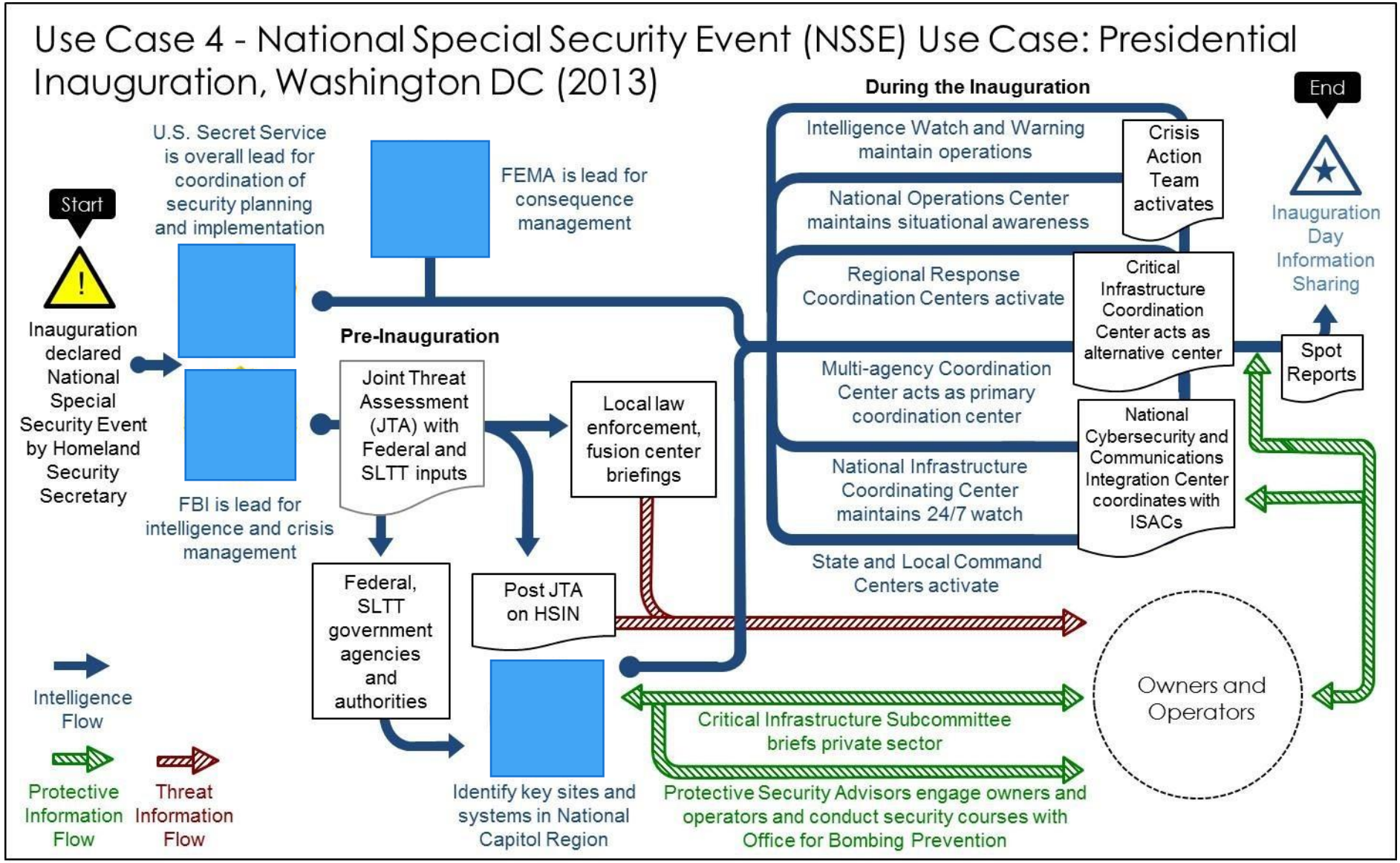
Польові операції I&A в Середньоатлантичному регіоні і Відділ розвідувального спостереження і попередження I&A підтримали цей захід, повідомляючи і передаючи інформацію про загрози, що виникали під час заходу, до штаб-квартири DHS, а також державним і місцевим партнерам, в тому числі, надаючи інформацію SPOTREP. Відділ польових операцій в Середньоатлантичному регіоні I&A також направив офіцерів розвідки до Центру контртерористичних операцій FBI (CTOC) і Центрів оперативного реагування на надзвичайні ситуації (EOC) у Вашингтоні, округ Колумбія, і Вірджинії з метою посилення підтримки і координації дій DHS з федеральними, державними, місцевими, племінними, територіальними партнерами і партнерами з приватного сектору під час проведення NSSE.

4.4.3.3 DHS - NCCIC

Національний координаційний центр (NCC) Національного центру інтеграції кібербезпеки і зв'язку (NCCIC) надав пряму і непряму підтримку інавгурації шляхом координації та співпраці з сектором зв'язку. Він також підтримував координацію і зв'язок між федеральними і галузевими членами Центру обміну і аналізу комунікаційної інформації (ISAC) (який входить до складу NCC) щодо оперативних питань і інцидентів, які викликають занепокоєння.

4.4.3.4 DHS - NOC

Національний оперативний центр (NOC) відстежував події інавгурації на рівні обізнаності з 20 по 22 січня. Для надання підтримки в день інавгурації в NOC-Watch була задіяна Команда кризових дій (CAT) з особовим складом, адаптованим до конкретних подій.



Малюнок 12: Варіант використання 4 - Національна подія особливої важливості (NSSE): Інавгурація президента, Вашингтон, округ Колумбія (2013)

Список скорочень

AIS - Автоматичний обмін індекаторами

AMSC – Берегова охорона США – Міністерство внутрішньої безпеки

AMSP – План морської безпеки району

AOR – Сфери відповідальності

ATIX – Автоматизований довірений обмін інформацією

C3 – Кіберспільнота критичної інфраструктури

CAT – Група кризових дій

CBAT – Комп'ютерний інструмент оцінювання (тепер Платформа візуалізації інфраструктури (IVP)

CCTV - Відеоспостереження

CG-FAC – Управління берегової охорони з відповідності портів і засобів

CICC – Координаційний центр критичної інфраструктури

CIF – Форум секретної розвідки для приватного сектора

CIG – Група кіберрозвідки фінансового сектору

CIMS – Система управління контактною інформацією

CIPAC – Консультативна рада партнерства з критичної інфраструктури

CIPSC – Підкомітет із захисту критичної інфраструктури

CISCP – Програма обміну кіберінформацією та співпраці

CMC – Центр антикризового управління

COP – Загальна робоча картина

COTP – Підпис до порту

CS&C – Управління кібербезпеки та комунікацій (Департамент внутрішньої безпеки)

CSA – Радник з кібербезпеки

CSO – Начальник охорони

CTAB – Консультативна рада з питань боротьби з тероризмом

CTOC – Антитерористичний оперативний центр

DFIR – Щоденний польовий інформаційний звіт (раніше – Стратегічний звіт про загрозу транспорту (STTAR)

DHS – Департамент внутрішньої безпеки

DOD – Департамент оборони

DOE – Департамент енергетики

DOJ – Департамент юстиції

DOT – Департамент транспорту

DSAC – Рада Альянсу внутрішньої безпеки

EEI – Електричний інститут Едісона

EOC – Центр екстреної допомоги

EPA – Агентство охорони навколишнього середовища

EWG – Робоча група із залучення
FAR – Звіт про польовий аналіз

FBI – Федеральне бюро розслідувань (Департамент юстиції)

FCC – Федеральна комісія зв'язку

FDA – Управління з контролю за харчовими продуктами та медикаментами

FEMA – Федеральне агентство з управління надзвичайними ситуаціями (Департамент внутрішньої безпеки)

FERC – Федеральна комісія з регулювання енергетики

FIO – Офіцер польової розвідки (Департамент внутрішньої безпеки)

FLASH - Система сповіщення ФБР

FOUO – Тільки для службового використання

FSLC - Федеральна рада вищого керівництва

GCC - Урядова координаційна рада

GSA - Адміністрація загального обслуговування

HHS - Охорона здоров'я та соціальні послуги

HMI - Людино-машинний інтерфейс

HSDN – Внутрішня мережа безпечної передачі даних

HSI - Розслідування внутрішньої безпеки

HSIN - Інформаційна мережа внутрішньої безпеки (Департамент внутрішньої безпеки)

I&A - Управління розвідки та аналізу (Департамент внутрішньої безпеки)

IC - Розвідувальна спільнота

IC3 - Центр скарг на злочини в Інтернеті (Федеральне бюро розслідувань)

ICS - Промислова система контролю

ICS-CERT – Промислова система контролю групи реагування на кібернетичні надзвичайні ситуації (Департамент внутрішньої безпеки, Управління кібербезпеки та зв’язку)

IED - Саморобний вибуховий пристрій

IEMC - Інтегрований курс управління надзвичайними ситуаціями

IIB - Відділення інтеграції розвідки

IIR - Інформаційний звіт розвідки

IO - Офіцер розвідки

IP - Управління захисту інфраструктури (Департамент внутрішньої безпеки, Управління національного захисту та програм)

ISA-IPC - Міжвідомчий комітет з політики обміну інформацією та доступу

ISAC - Центр обміну та аналізу інформації

ISAO - Організація обміну інформацією та аналізу

ISAO-SO - Організація обміну інформацією та аналізу – Організація стандартів

ISC - Міжвідомчий комітет безпеки

ISE - Середовище обміну інформацією

IST - Інструмент дослідження інфраструктури (Департамент внутрішньої безпеки)

IT - Інформаційні технології

IVP - Платформа візуалізації інфраструктури (раніше Інструмент комп'ютерної оцінки [CBAT]) (Департамент внутрішньої безпеки)

IWW - Відділ спостереження та попередження розвідки (Департамент внутрішньої безпеки)

JCAT - Спільна група з оцінки боротьби з тероризмом

JCTAWS - Серія спільних семінарів з питань боротьби з тероризмом

JIB - Об'єднаний розвідувальний бюлетень

JTA - Спільна оцінка загрози

JTTF - Об'єднана оперативна група з боротьби з тероризмом

JWICS - Об'єднані всесвітні системи розвідувального зв'язку

LEEP - Портал правоохоронних органів (Федеральне бюро розслідувань)

LES - Правоохоронні органи чутливі

MACC - Міжвідомчий координаційний центр

MS-ISAC - Багатоштатний Центр обміну та аналізу інформації

NBEOC - Національний бізнес-центр з надзвичайних ситуацій (Департамент внутрішньої безпеки, Федеральне агентство з управління надзвичайними ситуаціями)

NCATS - Національна оцінка кібербезпеки та технічні служби

NCC - Національний координаційний центр комунікацій (Департамент внутрішньої безпеки)

NCCIC - Національний центр інтеграції кібербезпеки та комунікацій (Департамент внутрішньої безпеки, Управління кібербезпеки та комунікацій)

NCI - Національна рада центрів обміну та аналізу інформації

NCR - Регіон національної столиці

NCRIC - Регіональний розвідувальний центр Північної Каліфорнії

NCSC - Національний центр контррозвідки та безпеки

NCTC - Національний антитерористичний центр

NGO - Неурядова організація

NICC - Національний координаційний центр інфраструктури (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

NIPP - Національний план захисту інфраструктури

NIST - Національний інститут стандартів і технологій

NOC - Національний оперативний центр (Департамент внутрішньої безпеки)

NPPD - Управління національного захисту та програм (Департамент внутрішньої безпеки)

NRC - Комісія ядерного регулювання або Національний центр реагування

NS/EP - Національна безпека та готовність до надзвичайних ситуацій

NSI - Національна ініціатива звіту про підозрілу діяльність (SAR).

NSIS - Національна стратегія обміну інформацією

NSISS - Національна стратегія обміну та захисту інформації

NSSE - Особливий національний захід безпеки

NTIPA - Національне визначення загроз та оцінка пріоритетів

NWC - Національний центр спостереження (Департамент внутрішньої безпеки, Федеральне агентство з управління надзвичайними

ситуаціями)

OBP - Управління запобігання бомбардуванням (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

OCIA - Управління аналізу кібернетичної інформації та інфраструктури (Департамент внутрішньої безпеки)

OCIO - Офіс головного інформаційного директора

ODNI - Офіс директора національної розвідки

OE - Управління постачання електроенергії та енергетичної надійності (Департамент енергетики)

OEC - Управління екстреного зв'язку (Департамент внутрішньої безпеки)

OHSEC - Управління внутрішньої безпеки та координації надзвичайних ситуацій (Міністерство сільського господарства США)

OSAC - Консультативна рада з безпеки за кордоном

PCII - Захищена інформація критичної інфраструктури

PG&E - Тихоокеанський газ і електроенергія

PII - Особиста інформація

PIN - Повідомлення приватної промисловості

PM-ISE - Керівник програми для середовища обміну інформацією (Офіс директора національної розвідки)

PPD-21 - Політична директива президента 21

PSA - Радник із захисної безпеки (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

PSAP - Пункти відповіді з питань громадської безпеки

PSCD - Відділ координації захисної безпеки (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

PSHSB - Бюро громадської безпеки та внутрішньої безпеки (Федеральна комісія зі зв’язку)

RC3 - Регіональна координаційна рада консорціуму

RD - Регіональний директор (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

RE-ISAC - Нерухомість – Центр спільного використання та аналізу інфраструктури

RFI - Запит інформації

RISS - Регіональні системи обміну інформацією

RRAP - Регіональна програма оцінки стійкості (Департамент внутрішньої безпеки)

SAIC - Центр стратегічного аналізу та інформації

SAR - Повідомлення про підозрілу діяльність

SCC - Секторальна координаційна рада

SEAR - Рейтинг активності спеціального заходу

SECIR - Відділ взаємодії із зацікавленими сторонами та стійкості кіберінфраструктури (Департамент внутрішньої безпеки, Управління кібербезпеки та комунікацій)

SLTT - Державні, місцеві, племінні та територіальні

SLTTGCC - Координаційна рада штату, місцевого, племінного та територіального уряду

SME – Експерт у предметній галузі

SOC - Секретарський оперативний центр (охорона здоров’я та соціальне обслуговування)

SOP - Стандартна процедура

SOPD - Відділ секторальної роботи та програм (Департамент внутрішньої безпеки, Управління захисту інфраструктури)

SPOTREP - Звіти про події

SSA - Секторальне агентство

SSI - Конфіденційна інформація безпеки

STIX - Вираз структурованої інформації про загрози

STTAR - Стратегічний звіт про загрозу транспорту (тепер щоденний інформаційний звіт [DFIR])

SVTC - Безпечна відеоконференція

TAXII - Надійний автоматизований обмін індикаторною інформацією

TLP - Протокол світлофора

TRACE MOVI - Адміністрування транспортної безпеки Віддаленого доступу до секретних анклавів (MOVI — назва постачальника)

TS/SCI - Цілком секретна/конфіденційна розділена інформація

TSA - Адміністрація транспортної безпеки (Департамент внутрішньої безпеки)

TSC - Центр безпеки терористів (Федеральне бюро розслідувань)

TSOC - Оперативний центр Управління транспортної безпеки (TSA) (Департамент внутрішньої безпеки)

TTP - Тактика, прийоми та процедури

U//FOUO - Несекретно//Тільки для службового використання

US-CERT - Команда реагування на комп'ютерні надзвичайні ситуації США (Департамент внутрішньої безпеки, Управління кібербезпеки та зв'язку)

USCG - Берегова охорона США (Департамент внутрішньої безпеки)

USDA - Міністерство сільського господарства США

USG - Уряд Сполучених Штатів

USSS - Секретна служба США (Департамент внутрішньої безпеки)

WOW - Берегова охорона США – Міністерство внутрішньої безпеки

Додаток А: Федеральніопераційні центри[68, 69]

Федеральні міністерства та відомства використовують свої організаційні операційні/наглядові центри для забезпечення внутрішніх вимог щодо обміну інформацією, пов'язаної з безпекою критично важливої інфраструктури та ситуативною обізнаністю щодо її стійкості. Ці операційні центри також часто спілкуються безпосередньо з власниками та операторами у своєму секторі, хоча деякі з них спілкуються переважно під час катастроф. У таблиці нижче наведено їхні ролі, обов'язки таконтактні особи.

Агенція/Організація	Офіс/Центр	Ролі / обов'язки / сфера діяльності	Коли звертатися	Телефон/Електронна пошта	Веб-сайт
Міністерство енергетики (DOE)	Центр оперативного реагування на надзвичайні ситуації (EOC)	Оперативний центр забезпечує цілодобову ситуаційну обізнаність, оповіщення, попередження та сповіщення про події та інциденти, що впливають на простір місії Міністерства енергетики США/Національної адміністрації з ядерної безпеки.	24/7	Первинна точка доступу: (202) 586-8100 Розсекречено: doehqeoc@oem.doe.gov Секрет: doeeoc@doe.sgov.gov	https://nnsa.energy.gov/aboutus/ourprograms/emergencyoperationscounterterrorism/operationscenter
Міністерство охорони здоров'ята соціальних служб (HHS)	Центри з контролюта профілактики захворювань (CDC) Центр з надзвичайних ситуацій (EOC)	Центр надзвичайних ситуацій CDC слугує командним центром CDC для моніторингу реагування на надзвичайні ситуації у сфері громадського здоров'я в США та за кордоном. Працюючи цілодобово, EOC є центральним пунктом зв'язку для повідомлень про загрози громадському здоров'ю і підтримує Оперативний центр міністра охорони здоров'я і соціальних службСША.	24/7	800-CDC-INFO https://wwwn.cdc.gov/dcs/ContactUs/Form	http://www.cdc.gov/phpr/eoc.htm

[68] Вибрано з "*Функціональних взаємозв'язків безпеки та стійкості критичної інфраструктури*" - DHS, червень 2013 року, включаючи оновлену інформацію для цієї Рамкової програми, червень 2016 року.

[69] Федеральні галузеві операційні центри мають різні операційні моделі. Багато з них в першу чергу забезпечують внутрішні потреби відомства і не взаємодіють безпосередньо з власниками та операторами критичної інфраструктури, проте деякі з них взаємодіють. Додаткову інформацію див. в описах підрозділів.

Агенція/Організація	Офіс/Центр	Ролі / обов'язки / сфера діяльності	Коли звертатися	Телефон/Електронна пошта	Веб-сайт
Міністерство охорони здоров'ята соціальних служб (HHS)	Управління з контролю за продуктами та ліками США (FDA) Центр оперативного реагування на надзвичайні ситуації	Офіс з управління кризовими ситуаціями керує Центром надзвичайних ситуацій (EOC) FDA, активуючи Групу управління інцидентами, що базується в EOC, з розширеним штатом з відповідних центрів та офісів для моніторингу надзвичайних ситуацій, сортування скарг та попереджень, видачі завдань організаційним компонентам, координації загальних операцій реагування агентства та спілкування із зовнішніми партнерами, які звертаються за технічною таматеріальною підтримкою.	Великі катастрофи та надзвичайні ситуації	(866) 300-4374	http://www.fda.gov/AboutFDA/CentersOffices/OfficeofOperations/OfficeofCrisisManagement/ucm253409.htm
Міністерство внутрішньої безпеки (DHS)	Федеральне агентство з надзвичайних ситуацій (FEMA) Національний центр з надзвичайних ситуацій для бізнесу (NBEOC)	NBEOC - це нова віртуальна організація, яка слугує інформаційним центром FEMA для двостороннього обміну інформацією між зацікавленими сторонами з державного та приватного секторів у підготовці до катастроф, реагуванні на них та відновленні після них. Примітка: NBEOC працює лише під час великих катастроф та надзвичайних ситуацій.	Великі катастрофи та надзвичайні ситуації	FEMA-private-sector@dhs.gov FEMA-PSR@dhs.gov	http://www.fema.gov/private-sector
Міністерство внутрішньої безпеки (DHS)	Федеральне агентство з надзвичайних ситуацій (FEMA) Національний центр спостереженн я (NWC)	NWC підтримує збір та розповсюдження інформації до інциденту до Національного оперативного центру (NOC) МЗС США для розробки національної загальної оперативної картини (COP).	24/7	(202)-646-2828 FEMA-NWC@fema.gov	http://on.fema.net/COMPONENTS/ORR/RESPONSE/Pages/NationalWatchCenter.aspx (лише для DHS)

Агенція/Організація	Офіс/Центр	Ролі / обов'язки / сфера діяльності	Коли звертатися	Телефон/Електронна пошта	Веб-сайт
Міністерство внутрішньої безпеки (DHS)	Національний координаційний центр зв'язку (FDA) (елемент Національного центру інтеграції кібербезпеки та зв'язку [NCCIC])	Як частина NCCIC Міністерства безпеки США, NCC постійно відстежує національні та міжнародні інциденти та події, які можуть вплинути на екстрені комунікації. Інциденти включають не лише терористичні акти, але й природні явища, такі як торнадо, повені, урагани та землетруси. У випадках надзвичайних ситуацій NCC Watch очолює зусилля з реагування на надзвичайні ситуації та відновлення зв'язку в рамках Функції підтримки в надзвичайних ситуаціях № 2 Національної структури реагування на надзвичайні ситуації. У січні 2000 року Білий дім призначив NCC центром ISAC з питань телекомунікацій відповідно до президентської директиви № 63. NCC- Communications ISAC сприяє обміну інформацією про вразливості, загрози, вторгнення та аномалії між 24 федеральними агентствами та понад 50 представниками приватного сектору, включаючи власників критично важливої інфраструктури в довіреному середовищі, для підтримки комунікаційної місії NCC в галузі національної безпеки/готовності до надзвичайних ситуацій.	24/7 Повідомляйте про будь-які поточні або прогнозовані перебої зв'язку, загрози, вразливості та/або інші критичні проблеми та/або занепокоєння щодо зв'язку.	(703) 235-5080 Розсекречено: ncc@hq.dhs.gov Секрет: ncc@dhs.sgov.gov JWICS: ncc@dhs.ic.gov	www.dhs.gov/national-координаційний центр - телекомунікації
Міністерство внутрішньої безпеки (DHS)	Національний оперативний центр (НОЦ) NOC Watch I&A Intelligence Спостереження та попередження Філія (IWW)	Через NOC офіс забезпечує ситуаційну обізнаність і моніторинг ситуації в країні в режимі реального часу, координує інциденти та заходи реагування, а також, спільно з Управлінням розвідки та аналізу (I&A), Відділом розвідувального спостереження та попередження, видає поради та бюлетені щодо загроз національній безпеці, а також щодо конкретних заходів захисту.	24/7	(202) 282-8101 Державні та місцеві органи влади: (202) 282-9685 Запити на інформацію: DHS-SPS-RFI@hq.dhs.gov Співробітник NOC може відповісти на питання про поточні події і передати інформацію офіцерам розвідки МЗС, призначеним до об'єднаних центрів: NOC.State&Local@hq.dhs.gov	www.dhs.gov/about-координація та планування офісних операцій https://hsin.dhs.gov

				IA.IWW@hq.dhs.gov	

Агенція/Організація	Офіс/Центр	Ролі / обов'язки / сфера діяльності	Коли звертатися	Телефон/Електронна пошта	Веб-сайт
Міністерство внутрішньої безпеки (DHS)	Операційний центр Адміністрації транспортної безпеки (TSA) (TSOC)	TSOC - це сучасний оперативний центр, який працює 24 години на добу, безперервно обмінюючись інформацією з федеральними, державними, місцевими та племінними організаціями, пов'язаними з транспортом. Він слугує єдиним контактним пунктом для інцидентів і кризових ситуацій, пов'язаних з безпекою на всіх видах транспорту, і є основним інтерфейсом до NOC Міністерства внутрішніх справ США.	24/7	(703) 563-3236 TSOC.ST@dhs.gov	https://www.tsa.gov/file/inside-look-transportation-security-operations- center
Міністерство внутрішньої безпеки (DHS)	Національний центр реагування Берегової охорони США	Управління берегової охорони з питань дотримання вимог до портів та об'єктів (Комендант CG-FAC) розробляє та впроваджує програми для запобігання інцидентів, пов'язаних з безпекою, захистом та охороною навколишнього середовища в морській галузі, а також для захисту подальшої життєздатності морської транспортної системи. Звертайтеся до цього офісу з поточних питань щодо політики у сфері критичної інфраструктури. Щоб повідомити про інцидент на морських об'єктах критичної інфраструктури, включаючи розливи нафти і викиди хімічних речовин, після дзвінка за номером 911, зверніться до Національного центру реагування (NRC).	24/7	CG-FAC: (202) 267-2675 NRC: (800) 424-8802	http://www.nrc.uscg.mil/
Міністерство транспорту (DOT)	Центр управління в кризових ситуаціях (CMC)	CMC призначений для моніторингу транспортних систем та інфраструктури країни 24 години на добу, 7 днів на тиждень. У разі стихійного лиха він слугує міжвідомчим зв'язком Міністерства оборони з федеральним урядом та урядами штатів і територій, де це необхідно.	24/7	(202) 366-1863 cmc-01@dot.gov	https://www.transportation.gov/mission/administrations/intelligence-security-emergency- response/operations- division
Агентство з охорони навколишнього середовища (EPA)	Центр управління в надзвичайних ситуаціях (EOC)	Центр надзвичайних ситуацій EPA (EOC) слугує оперативним координаційним центромреагування на надзвичайні ситуації EPA. Це комунікаційний та координаційний центр, призначений для покращення управління даними та координації.	24/7	202-564-3850 eoc.epahq@epa.gov	http://www.epa.gov/emergency-response/emergency-operation-center

Агенція/Організація	Офіс/Центр	Ролі / обов'язки / сфера діяльності	Коли звертатися	Телефон/Електронна пошта	Веб-сайт
Федеральна комісія зв'язку (FCC)	Оперативний центр Бюро громадської та національної безпеки (PSHSB)	Оперативний центр PSHSB забезпечує цілодобову ситуаційну обізнаність і стратегічну оцінку тенденцій щодо кризових сценаріїв, які можуть мати наслідки для громадської безпеки, національної безпеки або готовності до надзвичайних ситуацій, а також слугує основним центром зв'язку для FCC. Онлайн-портал Центру підтримки громадської безпеки дозволяє пунктам реагування громадської безпеки (PSAP), також відомим як колл-центри 911, та іншим суб'єктам громадської безпеки звертатися за підтримкою до Бюро громадської безпеки та внутрішньої безпеки і повідомляти його про проблеми або питання, що впливають на надання екстрених послуг.	24/7	Несекретно: (202) 418-1122 TS/SCI STE: (202) 418-1192 TS/SCI FAX: (202) 418-0908 Несекретно: FCCOPCenter@fcc.gov Секретно: FCCOPS@adnet.sgov.govTS: FCCOPS@gold.ic.gov	Операційний центр FCC https://www.fcc.gov/general/operations-center-public-safety-homeland-security-bureau Центр підтримки громадської безпеки https://www.fcc.gov/general/public-safety-support-center
Міністерство сільського господарства США (USDA)	Операційний центр Відділу надзвичайних програм	Відділ програм з надзвичайних ситуацій керує Оперативним центром, який є головним центром управління та координації всіх надзвичайних ситуацій у штаб-квартирі USDA. Центр відстежує міжнародні, національні та місцеві новини на предмет подій, які можуть вплинути на діяльність USDA, і є основною точкою входу USDA для отримання інформаціїпро надзвичайні ситуації від операційних центрів, що не входять до складу USDA.	24/7	(202) 720-5711 Запит на з'єднання з керівником продовольчого/сільськогос-подарського сектору в Управлінні внутрішньої безпеки та координації в надзвичайних ситуаціях Міністерства сільського господарства США (OHSEC) opscenter@dm.usda.gov	http://www.dm.usda.gov/ohsec/epd/
Комісія ядерного регулювання США (NRC)	Операційний центр NRC	Основний центр комунікації та координації між NRC, її ліцензіатами, державними та племінними установами, а також іншими федеральними агентствами щодо експлуатаційних подій, пов'язаних з ядерними реакторами або матеріалами.	24/7	(301) 816-5100 HOO.HOC@nrc.gov	http://www.nrc.gov

Додаток B: Інші організації, що обмінюються інформацією про загрози, невключені до Розділу 3.0 або Додатку A

Сутність	Ролі / обов'язки / сфера діяльності	Телефон/Електронна пошта	Веб-сайт
Група кіберрозвідки фінансового сектору (CIG)	CIG відстежує та аналізує розвідувальні дані з усіх джерел щодо кіберзагроз фінансовому сектору; надає сектору своєчасну, дієву інформацію про кіберзагрози; а також запитує відгуки та вимоги до інформації від сектору.	cig@treasury.gov	
Офіс програмного менеджера з питань середовища обміну інформацією (PM-ISE)	Роль PM-ISE полягає в координації та сприянні розвитку мережевого середовища обміну інформацією про тероризм та внутрішню безпеку, зосереджуючись на стандартах та архітектурі, безпеці та доступі, пов'язаному з цим захисті приватності та передовому досвіді. PM-ISE виступає агентом змін і центром інновацій та відкриттів, надаючи ідеї, інструменти та ресурси партнерам місії, які потім застосовують їх у своїх відомствах або громадах.	(202) 331-4060 ISE-public-affairs@dni.gov	www.ise.gov
Відділ управління загрозами	Відділ управління загрозами Федеральної служби охорони надає партнерам місії, орендарям і зацікавленим сторонам аналіз поточних і майбутніх загроз для державних об'єктів та їхніх мешканців по всій країні на основі аналізу загроз, орієнтованого на конкретні завдання місії.	202-732-8200 FPS-INTEL@hq.dhs.gov	
Національна оперативна група з вибухових речовин (NETF)	Місія NETF - координувати швидку інтеграцію експертних знань про вибухові речовини з розвідувальною та правоохоронною інформацією з метою підтримки оперативних рішень осіб, відповідальних за запобігання використанню вибухових речовин у терористичних або злочинних цілях. NETF має три основні цілі: підвищити рівень обізнаності у сфері вибухових речовин на національному рівні, інтегрувати розвідувальну інформацію та експертний досвід у розслідування, а також координувати публікації, пов'язані з саморобними вибуховими пристроями (IED). NETF підтримує підхід "всього уряду" для усунення прогалин у координації та консолідації зусиль у реагуванні на інциденти, пов'язані з вибуховими речовинами. NETF також співпрацює з Об'єднаним програмним офісом з протидії саморобним вибуховим пристроям з метою узгодження своєї місії, ресурсів і досвіду з Політичною заявою США щодо протидії саморобним вибуховим пристроям. До складу NETF входять вибухотехніки, слідчі та аналітики розвідки з FBI, Бюро алкоголю, тютюну, вогнепальної зброї та вибухових речовин, Управління запобігання вибухам Міністерства внутрішньої безпеки та Адміністрації транспортної безпеки, Національного контртерористичного центру при Директораті національної розвідки, Міністерства оборони та Аналітичного центру з питань терористичних вибухових пристроїв.	NETF@ic.fbi.gov	

Додаток С: Суб'єкти, відповідальні за програми, політику та управління безпекою та стійкістю критичної інфраструктури

Окрім суб'єктів обміну інформацією про загрози, перелічених у Розділі 2.2, та суб'єктів, перелічених у Додатках А та Б, існують суб'єкти, які несуть значну відповідальність за політику та програми, пов'язані з безпекою та стійкістю критично важливої інфраструктури. Вони координують свою діяльність зі спільнотою об'єктів критичної інфраструктури та розробляють або координують розробку стратегій, політик, планів та стандартів для забезпечення безпеки та стійкості об'єктів критичної інфраструктури. Під час підвищених загроз або реагування на інциденти вони можуть виступати в ролі профільних експертів в організаціях, які в основному відповідають за обмін інформацією про загрози та її аналіз. Вони також можуть координувати і розробляти ресурси та інструменти для допомоги власникам і операторам критичної інфраструктури у протидії новим загрозам. Як правило, ці організації є споживачами інформації, що надається вищезгаданими центрами обміну інформацією, і можуть надавати інформацію до центрів обміну інформацією або отримувати її від них. У деяких випадках вони також можуть ділитися інформацією про загрози безпосередньо із зацікавленими сторонами до або під час інциденту, але цілодобовий "обмін інформацією про загрози" не є одним з їхніх основних обов'язків. Цей додаток не є вичерпним.

Сутність	Ролі / обов'язки / сфера діяльності	Телефон/Електронна пошта	Веб-сайт
Добровільна програма Кібер-спільноти критичної інфраструктури (C3)	Добровільна програма C3 - це інноваційне державно-приватне партнерство, очолюване Міністерством національної безпеки США, покликане допомогти власникам і операторам об'єктів критичної інфраструктури отримати доступ до наявних ресурсів, які допоможуть їм використовувати Рамкову програму кібербезпеки Національного інституту стандартів і технологій (NIST) для управління своїми кіберризиками. Основним способом досягнення цієї мети є надання центрального сховища ресурсів на своєму веб-сайті та проведення вебінарів і заходів по всій країні.	CCubedVP@hq.dhs.gov	www.US-CERT.gov/CCubedVP

Сутність	Ролі / обов'язки / сфера діяльності	Телефон/Електронна пошта	Веб-сайт
Міністерство національної безпеки США - Управління національного захисту та програм (NPPD), відділ кібербезпеки та комунікацій (CS&C)	CS&C відповідає за підвищення безпеки, стійкості та надійності національної кібернетичної та комунікаційної інфраструктури. CS&C активно залучає державний і приватний сектори, а також міжнародних партнерів до підготовки, запобігання та реагування на катастрофічні інциденти, які можуть погіршити або вивести з ладу ці стратегічні активи. CS&C виконує свою місію через п'ятьпідрозділів, серед яких • NCCIC див. опис організації на сторінці 31 • Відділ взаємодії із зацікавленими сторонами та стійкості кіберінфраструктури (SECIR) та співробітники на місцях, радники з питань кібербезпеки (CSA). CSA діють як головні контактні особи на місцях у сфері кібербезпеки та надають федеральні ресурси регіонам, громадам і підприємствам. CSA співпрацюватимуть з існуючими програмами на рівні штатів і на місцевому рівні, такими як Радники з питань захисної безпеки (PSA), персонал Федерального агентства з надзвичайних ситуацій (FEMA) з управління в надзвичайних ситуаціях та персонал об'єднаних центрів. • Управління зв'язку в надзвичайних ситуаціях (OEC) підтримує і розвиває зв'язок, який використовується службами реагування на надзвичайні ситуації та державними службовцями, щоб забезпечити безпеку, захист і стійкість Америки. Офіс очолює національні зусилля з оперативного та оперативно-сумісного зв'язку у сфері громадської безпеки, національної безпеки та готовності до надзвичайних ситуацій (НС/ГН). OEC забезпечує навчання, координацію, інструменти та керівництво, щоб допомогти своїм партнерам на федеральному рівні, рівні штатів, місцевому, племінному, територіальному та галузевому рівнях розвиватиїхні можливості зв'язку в надзвичайних ситуаціях.	Програма CSA: CSE@dhs.gov OEC: OEC@dhs.gov	https://www.dhs.gov/office-кібербезпека та комунікації
Управління захисту інфраструктури (IP) DHS-NPPD	IP очолює та координує національні програми та політику у сфері безпеки та стійкості критичної інфраструктури, а також налагодив міцні партнерські зв'язки з державним та приватним секторами. Офіс проводить та сприяє проведенню оцінок вразливості та наслідків, щоб допомогти власникам та операторам об'єктів критичної інфраструктури, а також партнерам на державному, місцевому, племінному та територіальному рівнях (SLTT) зрозуміти та усунути ризики для критичної інфраструктури. IP надає інформацію про нові загрози та небезпеки, щоб можна було вжити відповідних заходів. Офіс також пропонує партнерам інструменти і тренінги, які допомагають їм управляти ризиками для їхніх активів, систем і мереж. IP виконує свою місію через п'ять підрозділів, які включають Національний інфраструктурний координаційний центр (NICC) та польовий персонал радників з питань захисної безпеки (PSA). Для отримання додаткової інформації відвідайте веб-сайт IP.		https://www.dhs.gov/office-інфраструктура-захист

Сутність	Ролі / обов'язки / сфера діяльності	Телефон/Електронна пошта	Веб-сайт
Національний центр контррозвідки та безпеки (NCSC)	NCSC очолює та підтримує інтеграцію контррозвідувальної та безпекової діяльності уряду США, Розвідувального співтовариства та суб'єктів приватного сектору, які перебувають під загрозою збору розвідувальних даних або проникнення іноземних чи інших супротивників. Іноземні супротивники становлять постійну загрозу для критичної інфраструктури США з можливістю завдати серйозної шкоди американській економіці та національній безпеці. NCSC відповідає за підготовку в консультаціях з відповідними урядовими департаментами і відомствами США та суб'єктами приватного сектору Національної оцінки ідентифікації та визначення пріоритетів загроз (NTIPA), яка забезпечує керівництво для програм і заходів, спрямованих на захист від іноземних проникнень в уряд США. Ініціативи NCSC включають програми протидії внутрішнім загрозам, управління ризиками ланцюгів постачання та інші заходи безпеки, що стосуються захисту критичної інфраструктури.		https://www.ncsc.gov/
Галузеві агентства (SSA)	Див. опис організації в Розділі 3 на сторінці 40		

Додаток D: Продукти для інформування про загрози

Цей додаток містить інформацію про низку різних специфічних інформаційних продуктів про загрози. Цей перелік не є вичерпним, але орієнтований на інформаційні продукти про загрози, на які спрямовані або які часто передаються власникам і операторам, або на довідкову інфраструктуру.

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Сповіщення - через портал ICS Національного центру інтеграції кібербезпеки та зв'язку (NCCIC) (розділ "Система управління") або портал корпоративних систем (розділ "Кобальт")	Сповіщення використовуються NCCIC та його партнерами,коли вони хочуть поділитися інформацією про рівень загрози, але працюють з розвідкою та правоохоронними органами, щоб обмежити обсяг інформації, яка може бути використана супротивниками.	NCCIC	U//FOUO або Засекречено	
Циркуляри Групи кіберрозвідки фінансового сектору (CIG)	Циркуляри CIG призначені для фахівців з мережевої безпеки фінансових установ, їхніх постачальників послуг з кібербезпеки та інших партнерів з критичної інфраструктури. Вони містять інформацію про тактику, методи, процедури та пов'язані з ними показники кіберзлочинців і використовуються для підтримки спроможностей мережевого захисту та планування.	Казначейство, Управління захисту критичної інфраструктури, Група кіберрозвідки фінансового сектору	Несекретно	http://fsisac.com Крім того, відповідні зацікавлені сторони можуть завантажити циркуляри CIG з порталу фінансових послуг Інформаційної мережі з питань національної безпеки (HSIN) Міністерства внутрішньої безпеки США. Для отримання інформації про членство завантажте короткий посібник за посиланням: http://go.usa.gov/3YH45
Щоденний звіт	Щоденні звіти складаються з використанням декількох постачальників розвідувальних даних з відкритим кодом і за передплатою. Після інцидентів вони можуть бути використані для інформування інших центрів обміну та аналізу інформації (ISAC) про загрози для членів, партнерів та інших секторів.	RE-ISAC	Несекретно	
Щоденний звіт DHS про інфраструктуру з відкритим кодом	Щоденний звіт Міністерства безпеки США з відкритих джерел щодо інфраструктури збирається кожного робочого дня як резюме опублікованої інформації з відкритих джерел щодо важливих питань критичної інфраструктури. Кожен щоденний звіт розділений за секторами критичної інфраструктури та ключовими активами, визначеними в Національному плані захисту інфраструктури.	DHS-IP	Несекретно	http://www.dhs.gov/publication/daily-open-source-infrastructure-report

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Інформаційний бюлетень (IB)	Інформаційні бюлетені (IB) - це універсальний аналітичний документ, який збирає і повідомляє ключову інформацію, що не є секретною. Інформаційний бюлетень охоплює широкий спектр тем, включаючи, але не обмежуючись ними, оцінку майбутніх подій, що впливають на федеральні об'єкти, та аналіз регіональних терористичних загроз.	Федеральна служба захисту DHS		
Брифінг з питань безпеки для керівників (ESB)	Брифінги керівництва з питань безпеки (ESBs) надають регіональному керівництву і зацікавленим сторонам аналітичну підтримку, яка покращує повсякденну діяльність, забезпечуючи ситуаційну обізнаність і підтримку в прийнятті рішень. Вони зосереджуються на наданні аналітичної підтримки для прийняття рішень щодо актуальних і специфічних загроз, пов'язаних з конкретнимитемами.	Федеральна служба захисту DHS		
Звіт про тероризм Міністерства безпеки США	Ці звіти розміщуються в Інформаційній мережі національної безпеки - критична інфраструктура (HSIN-CI) разом з Об'єднаними розвідувальними бюлетенями і звітами з польового аналізу. У них розглядаються зміни в загрозливих ситуаціях і підкреслюється необхідність бути пильними. Після інциденту один зі звітів містив аудіозапис телеконференції зацікавлених сторін у сфері критичної інфраструктури, яка надала уряду, власникам і операторам об'єктів інфраструктури можливість обмінятися інформацією про інциденти і конкретні загрози.	DHS-IP-NICC	Засекречені та незасекречені	
Повідомлення системи оповіщення FBI (FLASH)	FLASH використовується для обміну деталями та інформацією з приватним сектором. Повідомлення FLASHвикористовуються для надання партнерам з приватного сектору галузевої інформації про поточні та нові тенденції загроз і технічні показники.	FBI		З будь-якими питаннями, пов'язаними з повідомленнями FLASH, звертайтеся до FBI або до місцевої CTF, або до FBI CYWATCH: Електронна пошта: cywatch@ic.fbi.gov або Голос: +1-855-292-3937

Звіт про польовий аналіз (FAR)	FAR - це готові аналітичні продукти, які дозволяють проаналізувати загрози та впливи на критично важливу інфраструктуру в певному регіоні. Вони містять аналіз, заснований на фактах і дослідженнях, зібраних з технічних звітів з відкритих джерел, отриманих з різних урядових і неурядових джерел. Опубліковані в HSIN-CI, ці звіти, разом з Об'єднаними розвідувальними бюлетенями і Звітами про тероризм Міністерства безпеки США, розглядають ситуації підвищеної загрози і необхідність бути пильними. Приклади попередніх публікацій були використані для того, щоб надати уряду, власникам і операторам об'єктів критичної інфраструктури форум для обміну інформацією про інциденти і загрози. Деякі з попередніх публікацій включали аудіозаписи телеконференції зацікавлених сторін у сфері критичної інфраструктури.	DHS-I&A	Засекречені та незасекречені	

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Розвідувально-інформаційні звіти (IIR)	IIR публікуються Управлінням розвідки та аналізу (I&A) Міністерства національної безпеки США з метою надання детальної інформації про різні загрози, а також передаються розвідувальному співтовариству. Наприклад, Розвідувально-аналітичний відділ опублікував низку I&A, в яких детально описуються кампанії зловмисного програмного забезпечення, спрямовані проти об'єктів державного, місцевого та приватного секторів.	DHS-I&A	Засекречені та незасекречені	
Об'єднаний розвідувальний бюлетень (JIB)	JIB надає своєчасну інформацію або аналіз про нещодавню або поточну подію чи розвиток подій, що становлять інтерес. Вона надається замовникам інформації та аналізу і може бути підготовлена на різних рівнях засекреченості. Вона зосереджена на питаннях внутрішньої безпеки, пишеться на спеціальній основі і, якправило, має обсяг від однієї до трьох сторінок. Вона доступна в HSIN або в Homeland Secure Data Network (HSDN), залежно від рівня засекреченості інформації.[70]	FBI, DHS США	Різне	
Спільна оцінка загроз (JTA)	Спільні тактичні плани розробляються членами розвідувального співтовариства. JTA стосується міжнародних і внутрішніх терористичних, кримінальних, кібернетичних і транспортних загроз національним подіям і об'єктам спеціального призначення, пов'язаних з безпекою. Після підготовки JTA можуть бути передані федеральним, державним і місцевим органам влади та управління, щоб допомогти їм розробити і визначити пріоритетність заходів захисту і підтримки. JTA можна широко розповсюджувати серед власників/операторів об'єктів критичної інфраструктури NCR через HSIN, місцеві правоохоронні органи, об'єднані центри, а також на несекретних і секретних брифінгах.	FBI		
Національний антитерористичний центр (NCTC) Антитерористичний дайджест (CT Digest)	NCTC CT Дайджест - це збірник міжнародних і національних новин, присвячений інформації про боротьбуз тероризмом. Він доступний на сайтах HSIN-CI, InfraGard та Ради Альянсу внутрішньої безпеки (DSAC). CT Дайджест також містить оцінки від досвідчених аналітиків і фахівців з реагування на надзвичайні ситуації.	NCTC		Знайдіть на HSIN-CI, InfraGard та DSAC
Сповіщення приватного сектору (PIN-коди)	PIN-коди надають приватному сектору галузеву інформацію про поточні та нові тенденції загроз і технічні показники.	FBI		

[70] Посібник з розвідки для тих, хто першим реагує, 2nd видання, Міжвідомча група з оцінки та координації загроз (2011 р.).

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Повідомлення про підозрілу активність (SAR)	Загальнонаціональна ініціатива з SAR (NSI) - це спільна робота, яку очолює Міністерство юстиції США (DOJ), Бюро сприяння правосуддю, у партнерстві з Міністерством внутрішньої безпеки, FBI, а також партнерами з правоохоронних органів штатів, місцевих, племінних і територіальних органів влади. Ця ініціатива надає правоохоронцям ще один інструмент для запобігання тероризму та іншим пов'язаним з ним злочинам. Вона створює національний потенціал для збору, документування, обробки, аналізу та обміну інформацією про ПС. NSI - це стандартизований процес, що включає в себе роботу із зацікавленими сторонами, захист конфіденційності, навчання і сприяння розвитку технологій, для виявлення і повідомлення про підозрілу діяльність в юрисдикціях по всій країні, а також слугує єдиним координаційним центром для обміну інформацією про SAR.	Власники/оператори/ приватний сектор, DHS, FBI,закон SLTT партнери з право застосування	Засекречені та незасекречені	http://www.dhs.gov/how-do-i/report-suspicious-activity https://www.ise.gov/
Точкові звіти (SPOTREP)	Спот-звіти можна використовувати для обміну необхідною інформацією з NICC та операціями IP, а також для надання оновленої інформації про стан інцидентів, пов'язаних з критично важливою інфраструктурою.	DHS-IP-NICC	Засекречені та незасекречені	

Додаток E: Механізми та джерела інформації про загрози, а також інструменти для оцінки загроз

У цьому додатку міститься інформація про низку різних специфічних механізмів і джерел інформації про загрози. Ці специфічні джерела інформації доповнюють традиційний обмін інформацією через стандартні канали зв'язку, включаючи електронну пошту, особисті брифінги, телеконференції, бюлетені, звіти, веб-портали і центри надзвичайних операцій.

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Відсік для кобальту (US-CERT)	Cobalt Compartment - це захищений портал Національного центру інтеграції кібербезпеки та зв'язку (NCCIC) для обміну інформацією про кіберзагрози для корпоративних систем.	DHS-NCCIC		http://www.dhs.gov/publication/connecting-nicc-and-nccic
Відсік системи управління (ICS-CERT)	Відділ систем управління - це захищений портал NCCIC для обміну інформацією про кіберзагрози для власників та операторів промислових систем управління (ICS).	DHS-NCCIC		http://www.dhs.gov/publication/connecting-nicc-and-nccic
Форуми засекреченої розвідки (CIF)	CIF - це взаємодія з належним чином перевіреними та визначеними представниками критичної інфраструктури приватного сектору в рамках Сектору комерційних об'єктів та Міжсекторальної координаційної ради. Вони проводяться раз на два місяці в штаб-квартирі DHS США і були розширені на регіональному рівні для отримання зворотного зв'язку від представників приватного сектору, який може допомогти в розробці поточних і майбутніх розвідувальних продуктів та інших відповідних ініціатив з обміну інформацією або аналізу.	DHS I&A; DHS NPPD	Кілька класів, але зазвичай U//FOUO	
Щоденний звіт DHS про інфраструктуру з відкритим кодом	Щоденний звіт Міністерства безпеки США з відкритих джерел збирається кожного робочого дня у вигляді резюме опублікованої інформації з відкритих джерел, що стосується важливих питань критичної інфраструктури. Кожен щоденний звіт поділяється на сектори критичної інфраструктури та ключові активи, визначені в Національному плані захисту інфраструктури.	DHS-IP	Несекретно	http://www.dhs.gov/publication/daily-open-source-infrastructure-report
DHS - Відділ захисту інфраструктури (IP)	DHS-IP Desk знаходиться в Міжвідомчому координаційному центрі (MACC), який управляється Секретною службою Сполучених Штатів (USSS). Він слугує основним координаційним центром для діяльності радників з питань захисної безпеки (PSA) під час певних національних подій спеціальної безпеки (NSSE), а також забезпечує цілодобову підтримку обміну інформацією про загрози.	DHS-IP		

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Офіс головного офіцера з питань інформації Міністерства безпеки США	Інфраструктура геопросторової інформації Міністерства безпеки США (GII) забезпечує платформу рівня "чутливої, але несекретної інформації" (SBU) для розміщення спільних геопросторових корпоративних додатків, інструментів та інформації. Ця можливість, доступна всім користувачам у всій системі національної безпеки/оборони (на федеральному, штатному, місцевому рівні, рівні племен і територій), дозволяє операторам і аналітикам безпечно шукати, знаходити і отримувати доступ до знімків, базових карт, оперативних даних DHS і базових даних; зберігати і обмінюватися геопросторовою інформацією в приватних або публічних групах; створювати і обмінюватися похідними геопросторовими продуктами; отримувати доступ до існуючих загальних додатків і інструментів, таких як геокодування; а також з легкістю створювати інтерактивні мапи і індивідуальні додатки для польових досліджень, сюжетні мапи і теплові мапи.	DHS-OCIO	Несекретно	https://gii.dhs.gov/gii
Геопросторова концепція операцій національної безпеки (HSE Geo CONOPS)	HSE GeoCONOPS - це загальнодоступний ресурс, який дозволяє партнерам місій визначати наявні геопросторові ресурси і можливості для планування і підтримки місій (наприклад, план місії), легко шукати і знаходити геопросторові дані або продукти, доступні для їхньої місії, а також розуміти, як геопросторова спільнота взаємодіє/координує свою роботу для підтримки різноманітних місій за допомогою прикладів використання. За допомогою HSE GeoCONOPs аналітики можуть шукати, знаходити і використовувати іншу геопросторову інформацію про критично важливу інфраструктуру, доступну в інших відомствах.	OCIO МЗС США	Несекретно	https://cms.geoplatform.gov/geoconops/
eGuardian	eGuardian - це система відстеження терористичних загроз, яка підключена до Національної мережі об'єднаних центрів. eGuardian призначена для використання федеральними, державними, місцевими, племінними і територіальними правоохоронними органами, а також місцевими і державними об'єднаними центрами. eGuardian також використовується Міністерством оборони як єдиний механізм повідомлення про підозрілу активність. Відомства-учасники можуть надавати, переглядати і аналізувати звіти про підозрілу активність та іншу інформацію, пов'язану з тероризмом, використовуючи розширені пошукові можливості і геопросторові накладки.	FBI	Засекречені та незасекречені	https://www.fbi.gov/stats-services/eguardian
Електронна пошта	Електронна пошта є ключовим механізмом обміну інформацією. Можна підписатися на розсилку сповіщень, повідомлень, сповіщення про майбутній дзвінок про загрозутощо.	Кілька	Засекречені та незасекречені	

Робоча група із залучення (EWG)	EWG об'єднують потенційно постраждалих партнерів з приватного сектору та представників уряду для обговорення конкретної загрози або проблеми. Вони створюються для того, щоб доповнити типову роль Відділу інформаційно-просвітницької діяльності та програм (SOPD) Управління захисту інфраструктури (Office of Infrastructure Protection, IP), яка полягає у сприянні відносинам з приватним сектором через партнерство з Консультативною радою з питань партнерства у сфері критичної інфраструктури (Critical Infrastructure Partnership Advisory Council (CIPAC)).	DHS-IP-SOPD	Засекречені та незасекречені	

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Національна безпечна мережа передачі даних (HSDN)	HSDN дозволяє передавати секретну інформацію федеральним агентствам, які беруть участь у місіях з національної безпеки. HSDN - це засекречена глобальна мережа, яка використовується DHS, компонентами DHS та іншими партнерами, забезпечуючи ефективний взаємозв'язок з розвідувальним співтовариством і ресурсами федеральних правоохоронних органів. Homeland Secure Data Network (HSDN) надає DHS можливість збирати, поширювати та обмінюватися як тактичними, так і стратегічними розвідувальними даними та іншою інформацією з питань національної безпеки аж до рівня "Таємно". HSDN також слугує консолідованою магістраллю, яка об'єднує численні старі мережі з грифом "Таємно" по всьому підприємству Міністерства національної безпеки.	DHS - Офіс головного офіцера з питань інформації (OCIO)	Засекречено.	
Інформаційна мережа національної безпеки (HSIN)	HSIN - це мережа, якій довіряють оператори місій внутрішньої безпеки для обміну чутливою, але несекретною інформацією. Федеральні, державні, місцеві, територіальні, племінні, міжнародні та приватні партнери з внутрішньої безпеки використовують HSIN для управління операціями, аналізу даних, надсилання попереджень і повідомлень, і загалом для обміну інформацією, необхідною для виконання своєї роботи.	DHS	Несекретно	http://www.dhs.gov/homeland-security-information-network-hsin
Шлюз захисту інфраструктури (IP-шлюз)	IP-шлюз слугує єдиним інтерфейсом, за допомогою якого партнери DHS можуть отримати доступ до широкого спектру інформації та інтегрованих інструментів збору, аналізу та реагування на загрози для проведення комплексної оцінки вразливостей та аналізу ризиків. Він забезпечує єдину інтегровану систему, що спрощує доступ до інструментів захисту інфраструктури та наборів даних Міністерства.	DHS-IP		http://www.dhs.gov/ipgateway
Інструмент дослідження інфраструктури (IST)	IST - це веб-інструмент оцінки вразливості, що проводиться PSA, який застосовує зважені бали для виявлення вразливостей і тенденцій для конкретних об'єктів інфраструктури та всього сектору. Дані дослідження, що складаються із зважених балів за різними факторами для конкретної критичної інфраструктури, графічно відображаються на інформаційній панелі IST, яка порівнює дані з аналогічними об'єктами та надає інформацію для вжиття захисних заходів, планування стійкості та розподілу ресурсів. Інформація, отримана в результаті опитування, надається власникам і операторам, а також може бути передана галузевим відомствам та іншим представникам федеральних, державних, місцевих, племінних і територіальних органів захисту критичної інфраструктури через інтерактивні інформаційні панелі.	DHS-IP PSA		https://www.dhs.gov/sites/default/files/publications/ecip-ist-fact-sheet-508.pdf

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Платформа візуалізації інфраструктури (IVP) - колишній комп'ютерний інструмент оцінки (CBAT)	IVP - це засіб збору і представлення даних, який підтримує безпеку критичної інфраструктури, планування спеціальних заходів і операцій з реагування, використовуючи дані оцінки та інші відповідні матеріали. Інструмент інтегрує дані оцінки з імерсивним відео, геопросторовими та гіпермедійними даними об'єктів критичної інфраструктури, прилеглих територій і транспортних маршрутів, що допомагає співробітникам служб безпеки у плануванні, захисті та реагуванні на інциденти. Зображення IVP допомагають власникам і операторам інфраструктури, місцевим правоохоронним органам і персоналу служб реагування на надзвичайні ситуації готуватись до інцидентів з об'єктами критичної інфраструктури, NSSEs, спеціальних подій високого рівня та надзвичайних ситуацій, реагувати на них і керувати цими процесами. IVP готуються на запит власників та операторів об'єктів, місцевих правоохоронних органів та персоналу з реагування на надзвичайні ситуації через найближчу PSA. Залежно від обсягу зібраних даних, команді IVP зазвичай потрібно два тижні, щоб підготувати кінцевий продукт - DVD-диск із самозапускаючим програмним забезпеченням для презентацій, який надається представнику об'єкта, основній зацікавленій стороні Програми оцінки регіональної стійкості (RRAP) або персоналу, який планує безпеку під час спеціальних подій. Кінцеві продукти допомагають цим користувачам у навчанні, плануванні та прийнятті швидких і обґрунтованих рішень щодо готовності до інцидентів та управління ними.	УРП DHS-IP	FOUO або захищена інформація про критичну інфраструктуру (PCII)	https://www.dhs.gov/infrastructure-visualization-platform
Інтегрований курс з управління в надзвичайних ситуаціях (IEMC)	IEMC - це чотириденний курс, який є навчальною ініціативою, спрямованою на посилення спроможності місцевих органів влади захищати та реагувати на складні скоординовані атаки. Він включає в себе брифінги (в тому числі брифінг про загрози від Національного антитерористичного центру), тематичні дослідження та фасилітовані дискусії, засновані на сценарії нападу, характерному для конкретної громади. Під час обговорень на основі сценаріїв учасники самостійно визначають прогалини у своїх поточних операційних планах і можливостях, а також можливі рішення. Серед партнерів з приватного сектору - представники телекомунікаційних/мережевих провайдерів, комунальних служб, великих роботодавців - страхових, фінансових, виробничих, хімічних, логістичних та туристичних компаній, готелів, місць проведення спеціальних заходів, представників ділових кіл/палат у центрі міста, а також неприбуткових організацій - Американського Червоного Хреста, Волонтерських організацій, що беруть участь у ліквідації наслідків стихійних лих (VOAD), або релігійних мереж.	FEMA		https://training.fema.gov/iemc/

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Спільна серія семінарів з підвищення обізнаності про боротьбу з тероризмом (JCTAWS)	JCTAWS - це дводенний семінар для міст першого рівня. Він покликаний покращити спроможність місцевих юрисдикцій готуватись до комплексних терористичних атак, захищатись від них та реагувати на них. Він покликаний посилити спроможність місцевих юрисдикцій захищати від комплексних скоординованих атак та реагувати на них. Він включає в себебрифінги (в тому числі брифінг про загрози від Національного антитерористичного центру), тематичні дослідження та фасилітовані дискусії на основі сценаріїв атак, характерних для конкретної громади. Під час обговорення сценаріїв учасники самостійно визначають прогалини у своїх поточних оперативних планах і можливостях, а також шукають можливі рішення. З 2010 року семінар JCTAWS проводився 20 разів і зібрав понад 4500 учасників, серед яких були телекомунікаційні/мережеві провайдери, комунальні служби, великі роботодавці - страхові, фінансові, виробничі, хімічні, логістичні та туристичні готелі, місця проведення спеціальних заходів, представники ділових кіл/палат у центрі міста, а також неприбуткові організації - Американський Червоний Хрест, Волонтерські організації, що беруть участь у ліквідації наслідків стихійних лих (VOAD), або релігійні мережі.	NCTC; DHS; FBI		
Портал правоохоронних органів (LEEP)	LEEP - це онлайн-платформа, на якій FBI публікує розвідувальну інформацію, включаючи як готові розвідувальні дані, так і необроблену/тактичну інформацію. Ці ресурси допоможуть слідчим у розслідуванні справ, покращать обмін інформацією між відомствами та будуть доступні в одному централізованому місці.	FBI	Засекречені або незасекречені	https://www.cjis.gov/CJISEAI/EAIController
Регіональні системи обміну інформацією (RISS)	RISS пропонує безпечний обмін інформацією та комунікаційні можливості, критично важливі аналітичні послуги та послуги з підтримки розслідувань, а також послуги з деконфліктного врегулювання подій для підвищення безпеки офіцерів. RISS підтримує зусилля по боротьбі з організованою та насильницькою злочинністю, бандитизмом, наркобізнесом, тероризмом, торгівлею людьми, крадіжками особистих даних та іншими регіональними пріоритетами. RISS підтримує тисячі місцевих, державних, федеральних і племінних органів кримінального правосуддя в їхніх зусиллях щодо успішного вирішення кримінальних розслідувань і забезпечення безпеки офіцерів. RISS складається з шести регіональних центрів та Центру технологічної підтримки RISS.	Бюро сприяння правосуддю Міністерства юстиції США		www.riss.net

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Регіональні системи обміну інформацією (RISS) Автоматизований довірений обмін інформацією (ATIX)	RISS ATIX надає співробітникам правоохоронних органів, органів громадської безпеки та об'єктів критичної інфраструктури - таких як комунальні служби, школи, пожежні частини та хімічна промисловість - доступ до інформації про внутрішню безпеку, катастрофи та терористичні загрози, а також можливості захищеного зв'язку. В країні є шість регіональних центрів. Система RISS ATIX включає веб-сторінки, дискусійні форуми, захищену електронну пошту та бібліотеку документів, які можна використовувати для співпраці, обміну інформацією та доступу до ключових ресурсів.	Бюро сприяння правосуддю Міністерства юстиції США		www.riss.net/Resources/ATIX
Програма оцінки регіональної стійкості (RRAP)	RRAP - це спільна оцінка конкретних об'єктів критичної інфраструктури в межах визначеної географічної зони та регіональний аналіз навколишньої інфраструктури під керівництвом DHS- NPPD-IP. RRAP охоплює низку загроз, які можуть мати значні наслідки на регіональному та національному рівнях. Щороку Департамент відбирає ці добровільні, нерегулярні проекти RRAP за участю і під керівництвом федеральних і державних партнерів.	DHS-IP		https://www.dhs.gov/regional-resilience-assessment-program
Запит на інформацію (RFI)	У деяких випадках федеральні агенції просять Центри обміну та аналізу інформації (ISAC) ділитися з їхніми членами незасекреченою інформацією та інформацією з відкритих джерел. Крім того, власникам і операторам може бути запропоновано поділитися з ISAC будь-якою інформацією, що стосується справ, які вони мають у своєму розпорядженні.	ISAC	Несекретно	
Робочі групи з обміну інформацією в секторах та підсекторах	Існує багато робочих груп, які беруть участь в обміні інформацією, як державних, так і приватних. Одним з прикладів є Робоча група з обміну інформацією про сектор гребель, але це узагальнена категорія, яка ілюструє різноманітність та децентралізацію, притаманну обміну інформацією.	Різне	Засекречені та незасекречені	
Галузеві семінари та конференції	Ці семінари та конференції є форумом для особистого обміну інформацією. Вони об'єднують зацікавлені сторони з усього спектру державних установ федерального рівня, рівня штатів, місцевих, племінних і територіальних органів влади, а також приватного сектору. Вони підтримують презентації, брифінги та особисте спілкування щодо конкретних загроз або заходів з пом'якшення наслідків. Одним із прикладів є Саміт з безпеки хімічного сектору, але це загальна категорія, яка ілюструє різноманітність і децентралізацію, притаманну обміну інформацією.	Різне	Несекретно	
Секторні брифінги щодо загроз	Такі брифінги про загрози проводяться різними державними установами та відомствами. Вони є засобом обміну відповідною інформацією про загрози та висновками з власниками та операторами приватного сектору в часи підвищеної обізнаності.	Різне	Засекречені та незасекречені	

Назва джерела	Опис	Організація-виробник	Класифікація	Веб-сайт
Безпечна відеоконференція (SVTC)	Безпечні відеоконференції надають державним установам механізм для проведення розмов та брифінгів в режимі реального часу для обміну інформацією з іншими державнимиустановами та приватним сектором у разі потреби.	Урядові установи, включаючи DOE та DHS - NICC	Засекречено.	
Спеціальні тематичні та цільові завдання	Спеціальні тематичні та цільові завдання визначаються керівництвом IC і проводяться на різних рівнях, як правило, уразі виявлення інциденту, спрямованого на певний сектор. Ці завдання можуть бути як засекреченими, так і незасекреченими. Ці завдання можна класифікувати відповідно до Плану координації цільових завдань із реагування на загрози та забезпечення безпеки.	DHS-IP	Засекречені та незасекречені	
Цільові інформаційно-просвітницькі кампанії	Цільові інформаційно-просвітницькі кампанії визначені в Координаційному плані цільових заходів з протидії загрозам ібезпеки як один з багатьох типів заходів, що проводяться з приватним сектором. Ці заходи можуть бути як засекреченими, так і незасекреченими. Як правило, інформаційно-просвітницькі кампанії є широкомасштабними і проводяться по всій країні з метою інформування про загальнонаціональну загрозу.	DHS-IP та Міжгалузев а рада	Засекречені та незасекречені	
Телеконференція (Телеконференція зацікавлених сторін критичної інфраструктури, орієнтована на інциденти)	Ці телеконференції, що проводяться під керівництвом IC, надають уряду, власникам та операторам форум для обмінуінформацією про інциденти та загрози. За певних обставин аудіозаписи дзвінків передаються через HSIN-CI.	DHS-IP-NICC	Несекретно	
Віддалений доступ до засекречених анклавів Адміністрації транспортної безпеки MOVI (TRACE MOVI)	TRACE MOVI використовується державними установами для безпечного обміну секретною інформацією з іншими державними установами та ключовими партнерами з приватного сектору.	УПРАВЛІННЯ ТРАНСПОРТНОЇ БЕЗПЕКИ	Засекречено.	
TRIPwire (Технічний ресурс для запобігання інцидентам)	TRIPwire - це цілодобова мережа обміну інформацією Міністерства національної безпеки США, що працює в режимі 24/7, для вибухотехніків, спеціалістів служб швидкого реагування, військовослужбовців, урядовців, аналітиків розвідки та окремих фахівців з безпеки приватного сектору зметою підвищення обізнаності про тактику, методи і процедури використання терористами саморобних вибухових пристроїв (IED), а також про уроки, отримані в результаті інцидентів, та інформацію про готовність до протидії IED. Вінпоєднує експертний аналіз і звіти з відповідними документами, зображеннями і відео, зібраними безпосередньо з джерел, щоб допомогти користувачам передбачити, ідентифікувати і запобігти інцидентам з IED. TRIPwire - це захищена мережа обміну інформацією з обмеженим доступом, яка є безкоштовною для зареєстрованих підписників і має загальнодоступну домашню сторінку з цінною інформацією про готовність для всієї громади.	DHS-IP-Офіс із запобігання вибухам (OBP)	Несекретно	www.dhs.gov/tripwire https://tripwire.dhs.gov

Додаток F: Цільові загрози та завдання збезпеки[71]

Цільові загрози та заходи безпеки

Оскільки Управління захисту інфраструктури (IP) отримує інформацію про загрози від Розвідувального співтовариства (IC), в координації з міжгалузевими радами, IP перевіряє і визначає, чи є потреба в залученні сил безпеки, і в якому обсязі слід проводити роз'яснювальну роботу, щоб поділитися цією інформацією з відповідними власниками і операторами об'єктів критичної інфраструктури в державному і приватному секторі. Члени Міжгалузевої ради з питань критичної інфраструктури, Національної ради центрів обміну інформацією та аналізу (NCI), Регіональної координаційної ради консорціумів (RC3) та Координаційної ради штатів, місцевих, племінних і територіальних органів влади (SLTTGCC) також можуть звернутися до IC з проханням надати або запросити інформацію про нові загрози та/або проблеми, що виникають.

Як правило, в рамках цього процесу відбуваються наступні ключові кроки:

- IP та члени або представники Міжгалузевої ради з питань критичної інфраструктури, NCI, RC3, Федеральної ради вищого керівництва (FSLC) та SLTTGCC отримують інформацію про конкретні загрози.
  - Потенційними каналами отримання інформації про загрози є Управління розвідки та аналізу (I&A), засідання Контртерористичної консультативної ради (CTAB), Управління кібернетичного та інфраструктурного аналізу (OCIA), партнери з об'єктів критичної інфраструктури або інші канали.
- Робоча група з питань взаємодії (EWG) скликається для обговорення стратегії цілеспрямованої взаємодії з партнерами з критичної інфраструктури у постраждалому секторі та/або географічному регіоні.
- EWG, у координації з керівником напряму з питань IP, надає рекомендації Помічнику Секретаря (A/S) щодо необхідності та відповідних засобів для проведення цільових заходів.
- IP координує виконання стратегії взаємодії, затвердженої A/S, та повідомляє про це відповідних партнерів з державного та приватного секторів критичної інфраструктури.
- Для виконання завдань, пов'язаних із засекреченою інформацією про загрози табезпеку,

  IP робить два кроки:
  - Використовуйте різні варіанти, включаючи захищені засоби зв'язку та офіцерів зв'язку з урядом у місцях роботи зацікавлених сторін, для передачі секретних матеріалів допущеним до них одержувачам у промисловості та уряді.
  - Координуйте з Відділом внутрішнього аудиту розробку повідомлень з грифом "Для службового користування" (FOUO) та/або коротких повідомлень, щоб надати урядовим партнерам і членам Міжсекторальних рад дієві рекомендації таключові завдання, якими вони можуть поділитися зі своїми виборцями. Такі повідомлення можуть бути розроблені протягом розумного періоду часу після зустрічей з питань загроз і безпеки.
- Після завершення взаємодії, IP координуватиме свою роботу з Міжгалузевою радою з питань критичної інфраструктури, NCI, RC3, FSLC, SLTTGCC та іншими важливими об'єктами критичної інфраструктури.

[71] Управління захисту інфраструктури та міжсекторальних рад, *Координаційний план цільових заходів із захисту від загроз і безпеки*, (лютий 2016 р.).

Ми запрошуємо партнерів обговорити, чи була інформація корисною, а також визначити найкращі практики та уроки, винесені з цієї роботи (для використання в майбутніх проектах).

Періодичні завдання з питань загроз і безпеки

Періодично IP, у координації з I&A та OCIA, надаватиме партнерам з критично важливої інфраструктури інформацію про загрози та розвідувальну інформацію в рамках рутинної роботи з тестування і підтримки комунікаційних процесів та міжсекторальної обізнаності щодо ситуації в секторі.

Ця регулярна діяльність включатиме повідомлення всім відповідним партнерам, брифінг щодо загроз і розвідданих, обговорення і подальші дії для узагальнення отриманих уроків.

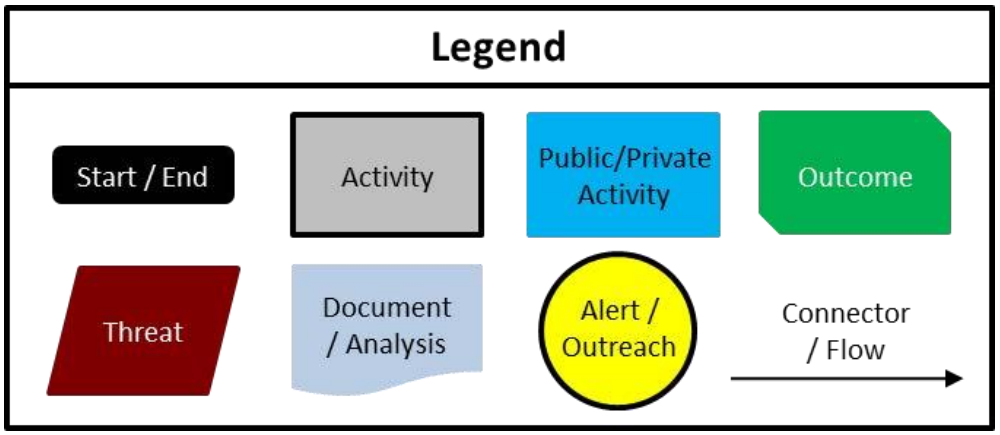
Ця співпраця надасть можливість Федеральному уряду, Міжгалузевій раді з питань критичної інфраструктури, NCI, RC3, SLTTGCC та іншим партнерам з критичної інфраструктури обмінюватися інформацією, продуктами, передовим досвідом та пріоритетами збору даних.

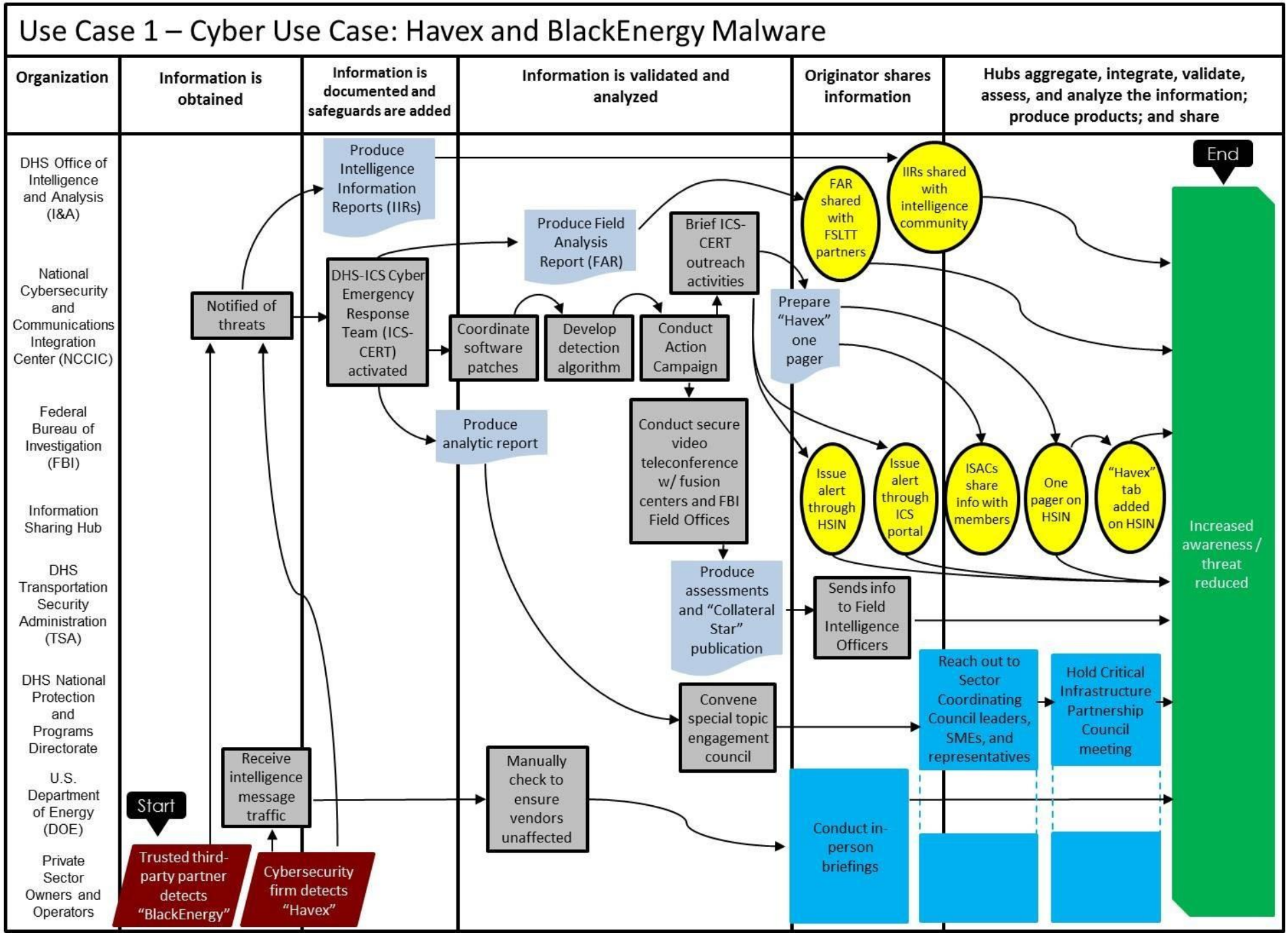
Ці зусилля забезпечать партнерів актуальною та доречною розвідувальною інформацією та інформацією про загрози, а також рекомендованими захисними заходами для зменшення ризиків. KI координуватиме свою діяльність з Міжгалузевою радою з питань критичної інфраструктури, NCI, RC3, FSLC, SLTTGCC та іншими партнерами з критичної інфраструктури, щоб забезпечити регулярне оновлення переліку належним чином перевіреного персоналу приватного сектору.

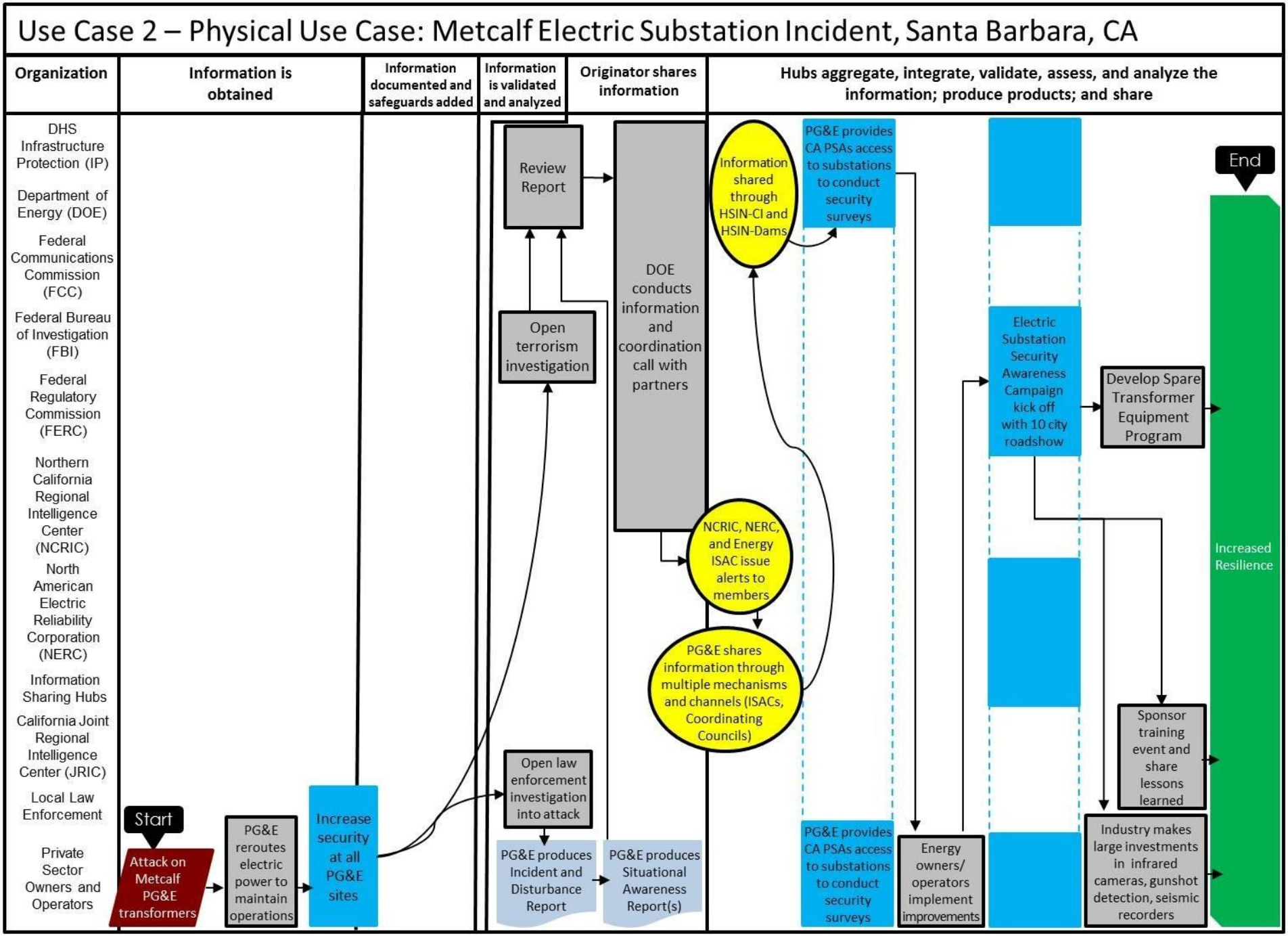
Цей процес також використовуватиметься для встановлення і підтримання контактів і відносин з партнерами по критичній інфраструктурі, щоб полегшити процес реагування на загрози і забезпечення безпеки в більш екстрених умовах.

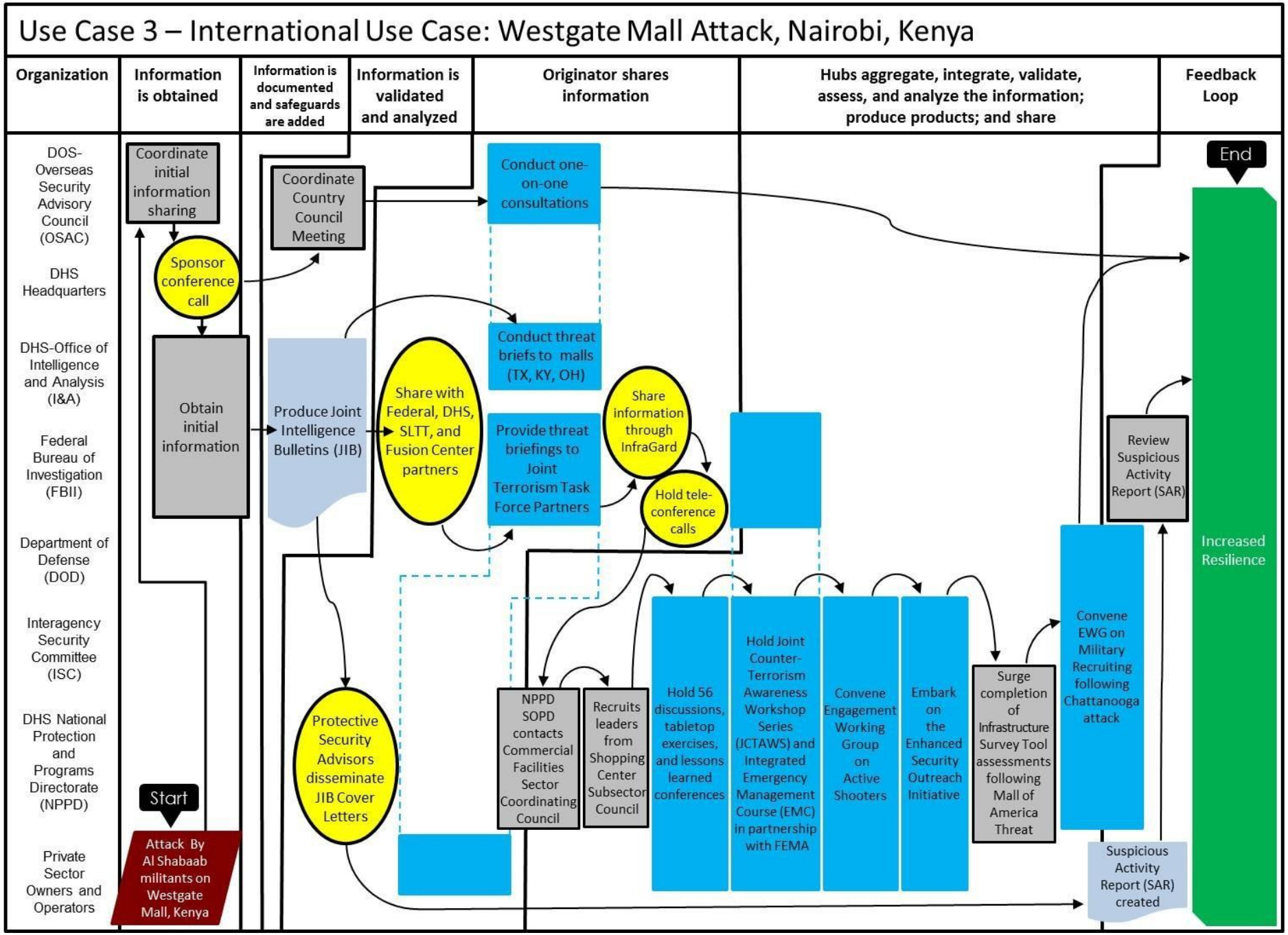
Додаток G: Карти інформаційних потоків варіантів використання

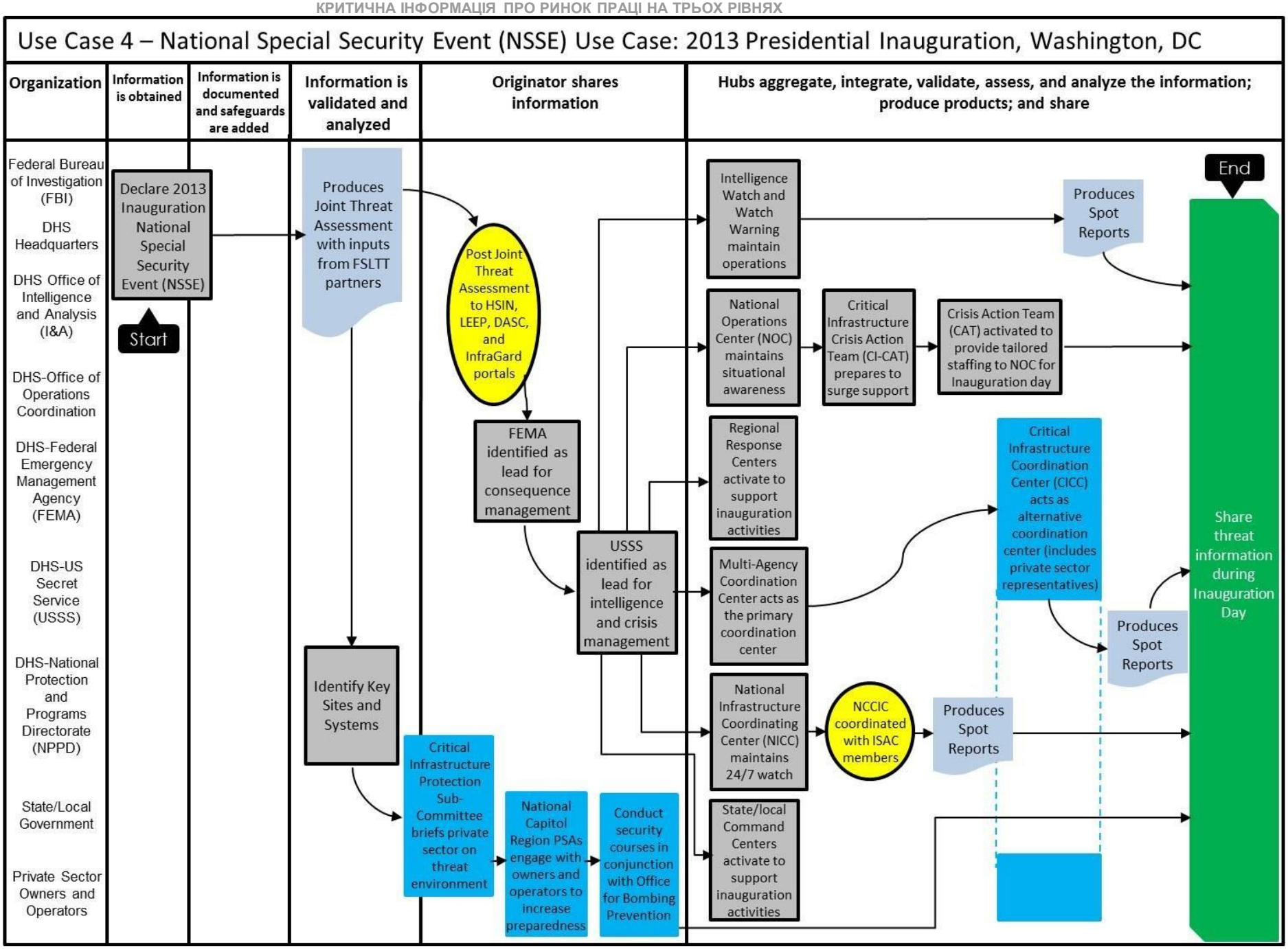
Ці карти потоків надають ще одну, більш детальну, візуалізацію інформаційних потоків у кожному з варіантів використання з Розділу 4.




Use Case 1 – Cyber Use Case: Havex and BlackEnergy Malware
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
DHS Office of Intelligence and Analysis (I&A)
National Cybersecurity and Communications Integration Center (NCCIC)
Federal Bureau of Investigation (FBI)
Information Sharing Hub
DHS Transportation Security Administration (TSA)
DHS National Protection and Programs Directorate
U.S. Department of Energy (DOE)
Private Sector Owners and Operators
Start
Trusted third-party partner detects "BlackEnergy"
Cybersecurity firm detects "Havex"
Receive intelligence message traffic
Notified of threats
Produce Intelligence Information Reports (IIRs)
DHS-ICS Cyber Emergency Response Team (ICS-CERT) activated
Produce Field Analysis Report (FAR)
Coordinate software patches
Develop detection algorithm
Conduct Action Campaign
Brief ICS-CERT outreach activities
Produce analytic report
Conduct secure video teleconference w/ fusion centers and FBI Field Offices
Manually check to ensure vendors unaffected
Produce assessments and "Collateral Star" publication
Convene special topic engagement council
FAR shared with FSLTT partners
IIRs shared with intelligence community
Prepare "Havex" one pager
Issue alert through HSIN
Issue alert through ICS portal
ISACs share info with members
One pager on HSIN
"Havex" tab added on HSIN
Sends info to Field Intelligence Officers
Conduct in-person briefings
Reach out to Sector Coordinating Council leaders, SMEs, and representatives
Hold Critical Infrastructure Partnership Council meeting
End
Increased awareness / threat reduced


Use Case 2 – Physical Use Case: Metcalf Electric Substation Incident, Santa Barbara, CA
Organization
Information is obtained
Information documented and safeguards added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
DHS Infrastructure Protection (IP)
Department of Energy (DOE)
Federal Communications Commission (FCC)
Federal Bureau of Investigation (FBI)
Federal Regulatory Commission (FERC)
Northern California Regional Intelligence Center (NCRIC)
North American Electric Reliability Corporation (NERC)
Information Sharing Hubs
California Joint Regional Intelligence Center (JRIC)
Local Law Enforcement
Private Sector Owners and Operators
Start
Attack on Metcalf PG&E transformers
PG&E reroutes electric power to maintain operations
Increase security at all PG&E sites
Review Report
Open terrorism investigation
Open law enforcement investigation into attack
PG&E produces Incident and Disturbance Report
DOE conducts information and coordination call with partners
PG&E produces Situational Awareness Report(s)
Information shared through HSIN-CI and HSIN-Dams
NCRIC, NERC, and Energy ISAC issue alerts to members
PG&E shares information through multiple mechanisms and channels (ISACs, Coordinating Councils)
PG&E provides CA PSAs access to substations to conduct security surveys
PG&E provides CA PSAs access to substations to conduct security surveys
Energy owners/ operators implement improvements
Electric Substation Security Awareness Campaign kick off with 10 city roadshow
Develop Spare Transformer Equipment Program
Sponsor training event and share lessons learned
Industry makes large investments in infrared cameras, gunshot detection, seismic recorders
End
Increased Resilience


Use Case 3 – International Use Case: Westgate Mall Attack, Nairobi, Kenya
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
Feedback Loop
DOS-Overseas Security Advisory Council (OSAC)
DHS Headquarters
DHS-Office of Intelligence and Analysis (I&A)
Federal Bureau of Investigation (FBII)
Department of Defense (DOD)
Interagency Security Committee (ISC)
DHS National Protection and Programs Directorate (NPPD)
Private Sector Owners and Operators
Coordinate initial information sharing
Sponsor conference call
Coordinate Country Council Meeting
Obtain initial information
Produce Joint Intelligence Bulletins (JIB)
Share with Federal, DHS, SLTT, and Fusion Center partners
Conduct one-on-one consultations
Conduct threat briefs to malls (TX, KY, OH)
Provide threat briefings to Joint Terrorism Task Force Partners
Share information through InfraGard
Hold tele-conference calls
Protective Security Advisors disseminate JIB Cover Letters
NPPD SOPD contacts Commercial Facilities Sector Coordinating Council
Recruits leaders from Shopping Center Subsector Council
Hold 56 discussions, tabletop exercises, and lessons learned conferences
Hold Joint Counter-Terrorism Awareness Workshop Series (JCTAWS) and Integrated Emergency Management Course (EMC) in partnership with FEMA
Convene Engagement Working Group on Active Shooters
Embark on the Enhanced Security Outreach Initiative
Surge completion of Infrastructure Survey Tool assessments following Mall of America Threat
Convene EWG on Military Recruiting following Chattanooga attack
Review Suspicious Activity Report (SAR)
Suspicious Activity Report (SAR) created
Start
Attack By Al Shabaab militants on Westgate Mall, Kenya
End
Increased Resilience


Use Case 4 – National Special Security Event (NSSE) Use Case: 2013 Presidential Inauguration, Washington, DC
Organization
Information is obtained
Information is documented and safeguards are added
Information is validated and analyzed
Originator shares information
Hubs aggregate, integrate, validate, assess, and analyze the information; produce products; and share
Federal Bureau of Investigation (FBI)
DHS Headquarters
DHS Office of Intelligence and Analysis (I&A)
DHS-Office of Operations Coordination
DHS-Federal Emergency Management Agency (FEMA)
DHS-US Secret Service (USSS)
DHS-National Protection and Programs Directorate (NPPD)
State/Local Government
Private Sector Owners and Operators
Declare 2013 Inauguration National Special Security Event (NSSE)
Start
Produces Joint Threat Assessment with inputs from FSLTT partners
Post Joint Threat Assessment to HSIN, LEEP, DASC, and InfraGard portals
FEMA identified as lead for consequence management
USSS identified as lead for intelligence and crisis management
Identify Key Sites and Systems
Critical Infrastructure Protection Sub-Committee briefs private sector on threat environment
National Capitol Region PSAs engage with owners and operators to increase preparedness
Conduct security courses in conjunction with Office for Bombing Prevention
Intelligence Watch and Watch Warning maintain operations
National Operations Center (NOC) maintains situational awareness
Critical Infrastructure Crisis Action Team (CI-CAT) prepares to surge support
Crisis Action Team (CAT) activated to provide tailored staffing to NOC for Inauguration day
Regional Response Centers activate to support inauguration activities
Multi-Agency Coordination Center acts as the primary coordination center
National Infrastructure Coordinating Center (NICC) maintains 24/7 watch
NCCIC coordinated with ISAC members
State/local Command Centers activate to support inauguration activities
Produces Spot Reports
Critical Infrastructure Coordination Center (CICC) acts as alternative coordination center (includes private sector representatives)
Produces Spot Reports
Produces Spot Reports
End
Share threat information during Inauguration Day

Homeland
Security