# DHS INTELLIGENCE SUBSCRIPTION

**DHS CONTRACT OVERVIEW**

U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA), purchased a three-year (Base Year plus two Option Years) subscription to FireEye Threat Intelligence (FireEye). The subscription began on 15 November 2017 and will end on 14 November 2020 if both Option Years are exercised. All Federal Civilian Agencies (FCAs) and State Fusion Centers are licensed to receive all FireEye Intelligence subscription products under this contract.

The Multi-State-Information Sharing Analysis Center (MS-ISAC) and Research Education Network-Information Sharing Analysis Center (REN-ISAC) are licensed to receive the FireEye Strategic subscription only.

**FIREEYE INTELLIGENCE OVERVIEW**

The FireEye subscription delivers comprehensive, non-classified, actionable intelligence to help organizations proactively defend against new and emerging cyber threats and align an organization's security program with its risk management goals. FireEye is tailored to an organization's security mission and staff and provides both mature and growing security teams critical context on attacker intent and activity. FireEye is unique in the industry. More than 150 FireEye security researchers and experts around the globe apply our rigorous intelligence process to collect, process, analyze and disseminate forward-looking, adversary-focused intelligence. FireEye has an unmatched view into adversaries, victims, and global networks and delivers visibility across the extended cyber-attack lifecycle to all levels of an organization's business through the FireEye subscription.

## FireEye Threat Intelligence Subscriptions

### FUSION INTELLIGENCE

Delivers comprehensive, situational awareness of the global threat landscape with insights into ongoing, past and predictive threat activity that covers cyber espionage, cybercrime, and hacktivism. It empowers cyber defense teams with a deep understanding of past, present and future adversary activities, including trends and typical tools, tactics and procedures (TTPs). The subscription equips organizations with processes, defense scenarios, deep dives and industry analyses to enable a proactive security posture. The subscription empowers advanced security operations centers (SOC) and incident response (IR) team members who proactively hunt for adversaries and want details about threat actors, their motives, and TTPs.

**Key Benefits:**

- Provides deep understanding into threat actors, their activities and TTP's
- Enables hunt missions to uncover attack patterns via technical and strategic intelligence
- Facilitates tracking actors and associated campaigns, incident trends and attribution indicators

### STRATEGIC* INTELLIGENCE

Conveys organizational risks to decision makers who direct security investment and strategy and includes intelligence analyses of industries, regions, and threats to enterprise networks. It improves executive-level communication on security topics relevant to an enterprise. Executive Intelligence is used by C-level executives, such as chief information security officers (CISOs), who want to understand the business risks associated with cyber threats.

**Key Benefits:**

- Improves executive-level communication on security topics relevant to the enterprise
- Provides focused intelligence analysis concentrated on threats targeting corporate networks
- Empowers independent organizational vision for intelligent security solutions

### VULNERABILITY INTELLIGENCE

Prioritizes patch management workflows based on active and evolving exploits of vulnerabilities in critical business systems. The subscription helps identify unaddressed vulnerabilities, prioritize patch cycles, increase patch effectiveness and more. Reports include all threat intelligence and vulnerabilities related to critical infrastructure. Vulnerability Intelligence is used by IT professionals and vulnerability analysts who want to improve efficiency and focus their time on top priorities.

**Key Benefits:**

- Empowers increased efficiencies in patching cycle via decisive knowledge of actively exploited vulnerabilities
- Provides expert analysis on regional propagation of code and ongoing malicious activity observed
- Includes all Critical Infrastructure related threat intelligence reporting and vulnerabilities

* The Executive subscription has been renamed to Strategic. The subscription content did not change.

## FireEye Threat Intelligence Deliverables

**FireEye Threat Intelligence Intelligence Portal (FIIP)** provides on-demand access to the complete online library of historical reporting for the subscription(s) purchased. Enablement Training to help successfully integrate and optimize FireEye Threat Intelligence usage. This training will provide DHS and all other organizations licensed under the subscription the ability to successfully integrate and optimize FireEye Threat Intelligence usage within their respective environments. Training can be tailored to an organization's specific use cases and can included some or all the following:

- FIIP overview
- API integration
- Forming intelligence requirements
- Leveraging threat intelligence for proactive SOC defense
- Leveraging threat intelligence for threat hunting and/or incident response
- Effective executive level communication leveraging threat intelligence
- Proactive patch management
- Leveraging threat intelligence without an intelligence team

**Email Alerts and Digests** deliver designated resources via email, as configured through FIIP. Threat Media Highlights delivers a daily report that tracks current security stories, answers inbound questions from business executives, and includes proactive analyses of important events to executives and board members. This report correlates media highlights with related FireEye Threat Intelligence Intelligence reports, handpicked by FireEye analysts, to provide a detailed and in-depth understanding of the security landscape.

**FireEye API** provides intelligence in automated, machine-to-machine formats (e.g. JSON, STIX, XML, CSV) that can be integrated into existing security technologies (e.g. SIEM, TIP, endpoint, IR, forensics, analytics) deployed in an organization.

**Browser Plugin** scans webpages for technical indicators (e.g., IP, domain, hashes) and queries the FireEye Threat Intelligence API for relevant intelligence report.

**Analysis Tools** enable the receipt of contextual information on domain names, IP addresses and threats, and allow for the upload of suspect files for analysis.

### How to Request FireEye Access

Send an email to fedinfo@fireeye.com. Use subject line "DHS Account Request" and include first name, last name and email (if different from the email requestor's address). *Please note that the email requesting FireEye Access MUST BE from an organization domain (e.g., state.gov, house.gov, uscourts.gov, etc.) licensed under the DHS license. All other requests will be rejected.

## FAQs

**Q:** Who can I contact to request enablement training for my staff/organization?

**A:** Please send the request to fedinfo@fireeye.com

**Q:** Who can I contact if I have a technical or analytical intelligence question and/or would like further information on an FireEye report?

**A:** This is considered an Analyst Access request and should be sent to analystaccess@fireeye.com.

**Q:** How can I submit IPs, domains and/or malware for analysis?

**A:** Submit these directly through the "Tools" section of FIIP. For additional analysis, open an Analyst Access request via analystaccess@fireeye.com.

**Q:** To which FireEye subscription(s) does each organization have entitlement?

**A:**
- FCAs and State Fusion Centers: Fusion, Strategic and Vulnerability.
- MS-ISAC and REN-ISAC: Strategic

**Q:** What is the scope of the FireEye license within the FCAs, MS-ISAC and REN-ISAC?

**A:** The license provides FireEye access to Federal Legislative, Judicial and Executive organizations, including the Independent Agencies under the Executive branch, MS-ISAC and REN-ISAC; however, the license does not include access to employees of the U.S. Department of Defense nor the Intelligence Community.

**Q:** With whom can I share FireEye Intelligence?

**A:** Any authorized FCA user may access and share FireEye information within their organization. The license does not include re-distribution rights, in any form, outside of the licensed organization. Standard limitations are further described at https://www.fireeye.com/company/legal.

To learn more about FireEye, visit: **www.FireEye.com**

**FireEye, Inc.**
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

**About FireEye, Inc.**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

FIREEYE™