The Enhanced Critical Infrastructure Protection (ECIP) initiative is a voluntary program which includes two parts: outreach and security surveys. Outreach establishes or enhances the Department of Homeland Security’s (DHS’s) relationship with critical infrastructure owners and operators and informs them of the importance of their facilities and the need for vigilance. Security surveys are conducted by the Office of Infrastructure Protection (IP) Protective Security Advisors (PSAs) to assess the overall security and resilience of the Nation’s most critical infrastructure sites.

**Program Description**

The primary goals of ECIP initiative and security surveys are to:

- Forge strong relationships among the owners and operators of the Nation’s most critical facilities, DHS, and Federal, State, local, tribal, and territorial partners. These relationships serve to increase communications and information sharing, enhance sector security, provide facility owners and operators access to Federal tools and resources.
- Inform and educate facility owners and operators about resilience and specific vulnerabilities and threats associated with the site or facility.

To accomplish these goals, PSAs leverage existing relationships and provide coordination for IP programs and resources to enhance protection and resilience efforts. These efforts include outreach, training and education, and recommended protective measures.

PSAs conduct voluntary ECIP security surveys in coordination with facility owners and operators, State Homeland Security Advisors, local law enforcement, sector-specific agencies (SSAs) that oversee the 16 critical infrastructure sectors, and other critical infrastructure partners such as industry organizations. ECIP security surveys accomplish the following:

- Identify facilities’ physical security, security forces, security management, protective measures, information sharing, dependencies, and capabilities related to preparedness, mitigation, response, resilience and recovery
- Create facility Protective and Resilience Measures Indices (PMI/RMI) that can be compared with similar facilities
- Inform planning and resource allocation for implementing protective and resiliency measures
- Track the implementation of new protective and resilience measures

The ECIP security surveys collect, process, and analyze facility assessment data in near real-time. Data collected during the ECIP security surveys is weighted and scored, enabling IP to conduct sector-by-sector and cross-sector vulnerability comparisons. These comparisons identify security gaps and trends and enable IP to track progress toward improving critical infrastructure security through its programs, outreach efforts, and training.
The resulting survey information is provided to owners and operators and may also be shared with the SSAs and other Federal, State, local, and private sector representatives through interactive “Dashboards.” In addition to providing a facility and sector security and resilience overview, the “Dashboards” highlight areas of potential concern and feature options to view the impact of potential enhancements to protective and resilience measures.

ECIP metrics provide DHS with information on the protective and resilience measures in place at facilities and enable detailed analyses of site and sector vulnerabilities. This approach serves as a mechanism for IP to identify and document critical infrastructure overall security, to provide information for protective and resiliency measures planning and resources allocation, to facilitate Government information sharing, and to enhance its ability to analyze data and produce improved metrics.

**Contact Information**

For more information, please contact [PDCDOperations@hq.dhs.gov](mailto:PDCDOperations@hq.dhs.gov).
The Computer Based Assessment Tool (CBAT) is a data collection and presentation medium designed to support critical infrastructure security, special event planning, and response operations. CBAT imagery captures provide immersive video, geospatial, and hypermedia data of critical facilities, surrounding areas, transportation routes, etc. and integrate assessment data from the Enhanced Critical Infrastructure Protection (ECIP) security surveys, Site Assistance Visits (SAVs), and other relevant materials. The data is used to support the Regional Resiliency Assessment Program (RRAP); National Special Security Events (NSSEs); other special events; and the initiatives of facility owners and operators, local law enforcement, and emergency response personnel. The CBAT’s final product is a DVD containing self-executing presentation software that is provided to the facility representative and/or the primary stakeholder of an RRAP or special event security planning personnel. The final products assist these users in planning and in making rapid and informed incident preparedness and management decisions.

Program Description

The CBAT is an essential tool for NSSEs, Special Event Activity Rating level events, and contingency operations. The Office of Infrastructure Protection collaborates with the United States Secret Service, the Federal Bureau of Investigation, and other agencies to conduct CBAT imagery collections. Examples of events supported by CBAT imagery captures include major league sporting events, Presidential debates and inaugurations, the Nuclear Security Summit, and the G8 Summit. CBAT is also used to prepare for the hurricane season by providing data collection and assessment data.

The CBAT team consists of collection and production specialists who conduct CBAT imagery captures. During a CBAT imagery capture, the CBAT team considers two viewpoints: hostile target and civil response. For the hostile target viewpoint, in which a facility/building is viewed as a tactical objective, the team collects multimedia data to document approach and exit routes, use of lighting, visible and hidden entrances, loading docks, and parking garages. In considering the civil response viewpoint, the team collects data on obstructions/restrictions that would affect the approach of emergency response vehicles and equipment to the site, and street/parking accessibility in proximity to building access points. Additional collected data include significant area assets such as exterior and interior critical support equipment (water valves, electrical shut-off panels, back-up generators, etc.), personnel emergency marshaling points, and control centers.

Contact Information

For more information, please contact: cbat@dhs.gov.
Preventing another terrorist attack in the United States continues to be one of the main missions of DHS. Ensuring that malicious actors cannot conduct terrorist attacks within the United States, and managing risks to our critical infrastructure and key resources, helps us realize our vision of a more secure and resilient Nation. In order to support this counterterrorism mission, each individual, business enterprise, and government agency must remain vigilant and report suspicious activity to law enforcement.

Suspicious Activity Reporting (SAR) is one of our best defenses against terrorist threats and our greatest resource to building resilience. Every day, members of the public work with law enforcement officers to help keep our communities safe by reporting activities that are out of the ordinary and suspicious. It is critical that law enforcement officers at all levels of government – state, local, tribal, territorial, and federal – who observe suspicious behaviors or receive reports from concerned civilians, private security, and other government agencies share this information with state and major urban area fusion centers, the Federal Bureau of Investigation, and other law enforcement agencies to help prevent future terrorist activity from occurring.

An aware and engaged public that understands what constitutes unusual and suspicious behavior is essential to protecting our communities from terrorist threats. For example, maybe you are at a high profile location or, perhaps a sporting event and you notice a person nearby taking several photos. While that is not unusual, you may also notice that the person is only taking photos of the locations of surveillance cameras, entrance crash barriers, and access control procedures. That type of activity would be unusual. The following are examples of other unusual activities that should cause a heightened sense of suspicion:

- Questioning individuals at a level beyond mere curiosity about particular facets of a facility’s or building’s purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person. Taking pictures or video of facilities, buildings, or infrastructure in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or video of infrequently used access points, personnel performing security functions (patrols, badge/vehicle checking), security-related equipment (perimeter fencing, security cameras), etc. Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.
- Abandoned packages constitute an implied threat due to the unknown nature of the contents. Unauthorized personnel attempting to or actually entering a restricted area or protected site. Impersonation of authorized personnel (e.g. police/security, janitor).

1 Information excerpted from the National Terror Alert Response Center.  
http://www.nationalterroralert.com/suspicious-activity/
• Presenting false or misusing insignia, documents, and/or identification, to misrepresent one’s affiliation to cover possible illicit activity.

• Stealing or diverting something associated with a facility/infrastructure (e.g., badges, uniforms, identification, emergency vehicles, technology or documents {classified or unclassified}, which are proprietary to the facility).

• Damaging, manipulating, or defacing part of a facility/infrastructure or protected site.

• Operation of an aircraft in a manner that reasonably may be interpreted as suspicious, or posing a threat to people or property. Such operation may or may not be a violation of Federal Aviation Regulations.

• Communicating a spoken or written threat to damage or compromise a facility/infrastructure.

• Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities.

• Demonstrating unusual interest in facilities, buildings, or infrastructure beyond mere casual or professional (e.g. engineers) interest such that a reasonable person would consider the activity suspicious. Examples include observation through binoculars, taking notes, attempting to measure distances, etc.

• Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would suspect possible criminal activity.

**Protective Measures**

Many different protective measures are available for deployment at a facility and in the areas surrounding a facility. Some are applicable to a wide range of facilities and against a number of threat streams, while others are designed to meet the unique needs of a specific facility or a specific threat stream. In addition, some may be tactical in nature, while others may address long-term strategic needs. Examples include:

**General Security**

- Restrict access to authorized personnel only; assign ID badges with photographs; ensure accountability for lock and key control
- Provide appropriate signs to restrict access to nonpublic areas.
- Have security personnel greet all employees and visitors and examine their personal belongings.
- Install a security/fire alarm system and associated security service; install CCTV to record operation area and exterior entrances.
- Ensure adequate lighting for the operations area, building exterior, and CCTV.

...
Screen all incoming mail offsite if possible; contact local law enforcement if a package is determined to be suspicious

Ensure accountability for lock and key control.

Develop an emergency plan for response to a known or a suspected hazard

Restrict drivers and deliveries to a specific area.

Establish a communication channel to report security deficiencies

Planning and Preparedness

- Designate an employee as a security director to develop, implement, and coordinate all security-related activities
- Develop a comprehensive security and emergency response plan
- Establish liaison and regular communication with local law enforcement
- Establish procedures to implement additional protective measures as the threat level increases

The DHS “If You See Something, Say Something™” Campaign

In July 2010, the Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" public awareness campaign—a simple and effective program to raise public awareness of indicators of potential terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts. To date, DHS has launched the "If You See Something, Say Something™" campaign in coordination with: Amtrak; the General Aviation community; the Washington, D.C. Metropolitan Police Department; the Washington Metropolitan Area Transit Authority (WMATA); the U.S. Tennis Association; the New York Mets; Meadowlands Stadium; the American Hotel and Lodging Association; New Jersey Transit; the Mall of America; Walmart; the National Football League (NFL); the National Basketball Association (NBA); NCAA and a variety of states.

For a full list of partnerships and for additional information about the campaign please go to www.dhs.gov/IfYouSeeSomethingSaySomething

The Office of Infrastructure Protection (IP) leads the national effort to mitigate risk to America's critical infrastructure from the full spectrum of 21st century threats and hazards. IP coordinates with government and critical infrastructure owners and operators across 18 diverse sectors to enhance critical infrastructure resilience, strengthen protective programs, and share vital information.
FACT SHEET
Office of Infrastructure Protection

Nationwide Suspicious Activity Reporting Initiative (NSI)
“If You See Something, Say Something™
State and Major Urban Area Fusion Centers

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)
The findings in the 9/11 Commission Report and the Markle Foundation report clearly demonstrated the need for a nationwide capacity to share information that could detect, prevent, or deter a terrorist attack. The Intelligence Reform and Terrorism Prevention Act (IRPTA) of 2004 and the 2007 National Strategy for Information Sharing indicate both legislative and executive intent to establish locally controlled, distributed information systems wherein potential terrorism-related information could be contributed by the 18,000 state, local, tribal, and territorial (SLTT) law enforcement agencies for analysis to determine whether there are emerging patterns or trends. Following this guidance, the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) was created. The NSI has established standards, policies, and processes for gathering, documenting, processing, analyzing, and sharing SAR while taking into account the protection of privacy, civil rights, and civil liberties of Americans. Behaviors that may not seem suspicious in and of themselves, when combined with other actions and activity, could be indicative of terrorist activity. The ability to share this information about suspicious activity is critical to law enforcement, from the officer on the street to supporting analysts. Through the efforts of the NSI – led by the U.S. Department of Justice and working in coordination with the Federal Bureau of Investigation and the Department of Homeland Security – the ad hoc methods of reporting and analysis cited in the 9/11 Commission Report have been standardized and policies and processes put in place so that timely, relevant information can be shared between state, local, tribal, and federal law enforcement agencies. For more information on the NSI please visit: http://nsi.ncirc.gov/.

The DHS “If You See Something, Say Something™” Campaign
In July 2010, the Department of Homeland Security (DHS), at Secretary Janet Napolitano's direction, launched a national "If You See Something, Say Something™" public awareness campaign – a simple and effective program to raise public awareness of indicators of potential terrorism and violent crime, and to emphasize the importance of reporting suspicious activity to the proper State and local law enforcement authorities. The campaign was originally used by New York's Metropolitan Transportation Authority (MTA), which has licensed the use of the slogan to DHS for anti-terrorism and anti-crime efforts. To date, DHS has launched the "If You See Something, Say Something™" campaign in coordination with: Amtrak; the General Aviation community; the Washington, D.C. Metropolitan Police Department; the Washington Metropolitan Area Transit Authority (WMATA); the U.S. Tennis Association; the New York Mets; Meadowlands Stadium; the American Hotel and Lodging Association; New Jersey Transit; the Mall of America; Walmart; the National Football League (NFL); the National Basketball Association (NBA); NCAA and a variety of states. For a full list of partnerships and for additional information about the campaign please go to www.dhs.gov/IfYouSeeSomethingSaySomething.
State and Major Urban Area Fusion Centers and Suspicious Activity Reporting

DHS works closely with the Department of Justice-led Nationwide Suspicious Activity Reporting Initiative Program Management Office to establish a standard process to identify and report suspicious activity in jurisdictions across the country. With the Office of Intelligence and Analysis (I&A) leading the way, DHS has made it a priority to participate in and support the implementation of the NSI while also integrating SAR processes across the National Network of Fusion Centers. The integration of NSI within both DHS and the fusion centers is a key element of coordinated outreach to homeland security stakeholder communities across the country.

Protective Security Advisors (PSAs) and the Enhanced Critical Infrastructure Protection (ECIP) Program

PSAs from the DHS Office of Infrastructure Protection, Protective Security Coordination Division, conduct security assessments and surveys of nationally significant critical infrastructure, known as Level 1 and Level 2 facilities, through the Enhanced Critical Infrastructure Protection (ECIP) program. The goals of the ECIP program are to assess overall security postures and recommend protective security measures at Level 1 and Level 2 facilities; to inform facility owners and operators of the importance of their facilities and threats from terrorism; and to develop strong relationships between critical infrastructure owners and operators, DHS, and Federal, State, Local, Tribal and Territorial law enforcement and intelligence communities. PSAs reside and work in communities across the country. They play a vital role in supporting National level homeland security initiatives such as the Nationwide Suspicious Activity Reporting, the DHS "If You See Something, Say Something™" Campaign, and the National Network of Fusion Centers by conducting outreach activities to educate and inform members of their stakeholder communities.
To reduce risk to the Nation’s critical infrastructure, the National Protection and Programs Directorate’s Office of Infrastructure Protection (NPPD/IP) maintains a catalog of training programs to develop awareness of terrorist threats to critical infrastructure among Federal, State, local, tribal, territorial and private sector entities. Coordinated through State Homeland Security Officials and training offices, the courses educate participants on strategies for detecting and mitigating threats. These courses may be requested by State, local, tribal, territorial agencies and critical infrastructure owners and operators through DHS Protective Security Advisors.

**Private Sector Counterterrorism Awareness Workshop**

This workshop trains private sector security professionals on key elements of improvised explosive device (IED) awareness, surveillance detection methods, and soft target awareness. The material presented illustrates important prevention actions that reduce vulnerabilities and provides information resources to improve preparedness. (One day, 100-250 participants)

**Bombing Prevention Workshop**

This workshop enhances knowledge of preventative measures and planning protocols to address IED threats. Participants, including regional public and private stakeholders, emergency management planners, and security enforcement personnel, review best practices for developing strategies or plans that require interagency collaboration across multiple localities, disciplines, and levels of government. The workshop concludes with a guided discussion, based on National Planning Scenario #12-Explosive Attack – IED Bombings, that establishes the foundation for regional stakeholders to implement a Bombing Prevention Plan. (One day, 50 participants)

**Improvised Explosive Device Awareness/Bomb Threat Management Workshop**

This workshop improves participants’ ability to manage IED threats by outlining specific safety precautions associated with explosive incidents and bomb threats. By reinforcing an integrated combination of planning, training, exercises, and equipment acquisition, this workshop maximizes available resources. (Four hours, 50 participants)

**Improvised Explosive Device Search Procedures Workshop**

This workshop enhances knowledge of IED awareness, prevention measures, and planning protocols by outlining specific search techniques that reduce vulnerability and mitigate IED attack risk. Culminating in a practical application of skills during which participants demonstrate search techniques, the workshop also emphasizes a team-building approach. (Eight hours, 25 participants)

**Soft Target Awareness Course**
This course provides an information-sharing venue for critical infrastructure personnel to discuss terrorism prevention and protection information to enhance individual and organizational security awareness. Participants learn the importance of engaging in proactive security measures and how to better define individual roles in deterring, detecting, and defending facilities from terrorist acts. (Five four hour sessions, 35 participants per session)

**Protective Measures Course**

This course teaches public and private sector security officers, mid-level safety and security supervisors, and property managers to identify vulnerabilities and employ appropriate protective measures dependent upon an individual facility’s design and operation. (Two days, 35 participants)

**Surveillance Detection Training for Municipal Officials, State and Local Law Enforcement Course**

This course, designed for municipal security officials and State and local law, tribal, and territorial enforcement with jurisdictional authority over Level 1 and Level 2 critical infrastructure facilities, provides participants with the skills and knowledge to establish surveillance detection operations to protect critical infrastructure during periods of elevated threat. Consisting of five lectures and two exercises, the course increases awareness of terrorist tactics and attack history, and illustrates the means and methods used to detect surveillance. (Three days, 25 participants)

**Surveillance Detection Training for Critical Infrastructure Operators and Security Staff Course**

This course, designed for critical infrastructure operators and security staff of Level 1 and Level 2 critical infrastructure facilities, provides participants with the skills and knowledge to establish surveillance detection operations to protect critical infrastructure during periods of elevated threat. Consisting of five lectures and two exercises, the course increases awareness of terrorist tactics and attack history, and illustrates the means and methods used to detect surveillance. (3 days, 25 participants)

**Improvised Explosive Device Counterterrorism Workshop**

This workshop is designed to enhance the knowledge of State and local law enforcement and public-private sector stakeholders by providing exposure to key elements of the IED threat, surveillance detection methods and soft target awareness. The workshop illustrates by illustrating baseline awareness and prevention actions, the workshop reduce vulnerabilities and counter threats by enabling information-sharing resources to improve preparedness. This designed approach better allows the owners and operators of critical infrastructure to deter, prevent, detect, protect against, and response to terrorist use of explosives. (4 to 8 hours, 100 to 250 participants)

For more information, please contact PSAFieldOperationsStaff@hq.dhs.gov.
TRIPwire Community Gateway (TWCG) is a TRIPwire web portal designed specifically for the Nation’s critical infrastructure owners, operators, and private security personnel. TWCG provides expert threat analyses, reports, and relevant planning documents to help key private sector partners anticipate, identify, and prevent improvised explosive device (IED) incidents.

Developed and maintained by the National Protection and Programs Directorate’s Office of Infrastructure Protection (NPPD/IP), TWCG shares IED-related information tailored to each of the 18 critical infrastructure sectors, as well as educational institutions in a community sector, in accordance with the National Infrastructure Protection Plan. Sector partners benefit from increased communication, improved awareness of emerging threats, and access to resources and guidance on specific IED preventive and protective measures. TWCG is available on the Homeland Security Information Network Critical Sectors (HSIN-CS) system.

**TRIPwire Community Gateway Benefits**
- Information sharing resources for all 18 NIPP Sectors and Community Sector;
- Searchable documents, resources, and profiles;
- Free access, provided by the Department of Homeland Security (DHS); and
- Secure access, limited to critical infrastructure partners.

**Expert Analysis and IED Awareness on**
- Significant Global Critical Infrastructure Incidents;
- Bombing Tactics;
- Critical Infrastructure Bombing Targets;
- Critical Infrastructure Common Vulnerabilities;
- Potential Indicators of terrorist activities; and
- Critical Infrastructure Bombing Protective Measures.

**Key Features include**
- Industry-Standard Foresight Reports;
- Bomb-making Materials Awareness Program Materials;
- Secure Email;
- Message Boards; and
- Feedback.

To become a member of HSIN-CS, please contact HSIN.Outreach@hq.dhs.gov for more information.
The Homeland Security Act of 2002\textsuperscript{1} was the governing document that officially formed the U.S. Department of Homeland Security (DHS) and mandated (among other things) that the department “… carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States.” In response to this mandate, in 2009, the DHS and its Protective Security Advisors began assessing nationally critical infrastructure assets using a targeted questionnaire, the Infrastructure Survey Tool (IST). The data collected was used to produce asset-specific protective measure information conveyed through the Protective Measures Index (PMI).

The main objective of the PMI is to provide a relative measure of the ability of a critical infrastructure asset to resist disruptive events—an indication of how well protected the asset is. The PMI has been formulated to capture the fundamental aspects of protection for critical infrastructure and facilitates the comparison of protection postures across critical infrastructure assets. Aggregate information can be used to assess prevalent sector and subsector security gaps, identify potential protective measures and enhancements to reduce potential vulnerabilities, and assist in preparing sector risk estimates.

The PMI methodology generates reproducible results that can support decisionmaking concerning critical infrastructure risk management. The PMI complements other indices that have been developed — the Resilience Measurement Index (RMI) and Consequences Measurement Index (CMI) — allowing a holistic view of most components of critical infrastructure risk.

The PMI aggregates five operational dimensions of protection as shown in Figure 1: Physical Security, Security Management, Security Force, Information Sharing, and Security Activity Background.\textsuperscript{2} The PMI calculation uses decision-analytic techniques with a basis and multi-attribute utility theory. The PMI ranges from 0 (low protection) to 100 (high protection) and is based on data collected via the IST that have been weighted by subject matter experts to indicate the relative importance of each variable to the asset’s overall protection posture.

Asset-specific protection information is displayed on a Web-based tool called the IST PMI Dashboard. The IST PMI Dashboard provides valuable information to owners and operators regarding their facility’s protection relative to similar assets.\textsuperscript{3} The Dashboard can be used to create scenarios and assess relative improvement of overall facility protection when specific protective measures and/or

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{PMI_Diagram.png}
\caption{Level 1 Components of the PMI.}
\end{figure}

---

\begin{itemize}
\item \textsuperscript{3} The data displayed for the facility is static, reflective of the relative resilience of the facility at the time of the survey.
\end{itemize}
procedures are added or changed. Policies, procedures, or operational methods are enhancements with which the facility may increase protection.

Figure 2 is a screenshot of the IST PMI Dashboard Overview Screen. The Overview Screen displays overall PMI as well as the five main components: Physical Security, Security Management, Security Force, Information Sharing, and Security Activity Background. The sets of three dots allow the user to visually compare their facility protection stature to the low, average, and high protection postures of comparable facilities. The Dashboard’s interactive “Facility Scenario” function allows the facility owner or operator to select possible protection enhancements and immediately see the resulting modified PMI (the light blue bars).

![Image of IST PMI Dashboard Overview Screen](Illustrative Asset)

The PMI should be used as part of an overall risk management program and can support decisionmaking about protection, business continuity, and emergency management of critical infrastructure. It provides important information about the protective measures implemented at a given facility and how that facility compares to similar facilities. Other factors such as location, specific vulnerabilities, and a cost-benefit analysis, should also be utilized to ensure a complete picture of a facility’s protection level or posture.

The asset-specific protection, used in conjunction with vulnerability information, and facility consequence and resilience information can provide decision makers with a comprehensive risk picture with which to make management and policy decisions ensuring the continued protection and resilience of our Nation’s critical infrastructure.
In 2009, the U.S. Department of Homeland Security (DHS) and its Protective Security Advisors began surveying critical infrastructure using the Infrastructure Survey Tool (IST.) The data collected was initially used to produce asset specific protective measure through the Protective Measures Index (PMI). As national priorities for critical infrastructure expanded beyond protection to include focus on resilience\(^1\), it became necessary to collect and display asset specific resilience-related information as well, resulting in the creation of the Resilience Measurement Index (RMI).

Resilience, in the context of critical infrastructure, can be defined as the ability of an entity (e.g., asset, organization, community, region) to anticipate, resist, absorb, respond to, adapt to, and recover from a disturbance.\(^2\) Enhancing the resilience of critical infrastructure requires its owners and operators to understand the ability of that infrastructure to withstand specific threats, minimize or mitigate potential impacts, and to return to normal operations if degradation occurs (threat to consequence.) The RMI has been formulated using decision-analytic techniques with a basis in multi-attribute utility theory, to capture the fundamental aspects of resilience for critical infrastructure.

The RMI is an aggregate measure of four operational dimensions that encompass the elements of that definition of resilience: Preparedness, Mitigation Measures, Response Capability, and Recovery Mechanisms (see Figure 1). The RMI, which ranges from 0 (low resilience) to 100 (high resilience), allows comparison of the resilience of different critical infrastructure assets and provides a basis for prioritizing the implementation of operational and physical enhancements to increase asset resilience.

Asset specific resilience information is displayed on an interactive, Web-based tool called the IST RMI Dashboard. The IST RMI Dashboard provides valuable information to owners and operators regarding

---


---

If you have further questions about the RMI, please contact DHS at PSCDOperations@hq.dhs.gov.
their facility’s resilience relative to similar assets\(^3\). The Dashboard can be used to create scenarios and assess the relative improvement of overall facility resilience when specific resilience measures and/or procedures are added or changed. Policies, procedures, or operational methods are enhancements with which the facility may increase resilience.

![IST RMI Dashboard](image)

**Figure 2.-RMI Dashboard Overview Screen (Illustrative Asset)**

Figure 2 is a screenshot of the IST RMI Dashboard Overview Screen used to display the results of a resilience analysis for a particular asset. Existing facility resilience values are indicated with dark blue bars. The Overview Screen displays overall RMI as well as the four main components of the RMI (Preparedness, Mitigation Measures, Response Capabilities, and Recovery Mechanisms). The sets of three dots allow the user to visually compare their facility resilience stature to the low, average and high resilience postures of comparable facilities (e.g., sector, subsector, segment). The Dashboard’s interactive “Facility Scenario” function allows the facility owner or operator to select possible resilience enhancements and immediately see the resulting modified RMI (the light blue bars).

The RMI methodology supports decisionmaking related to emergency management, disaster response, and maintenance of business continuity. It is most valuable as part of an overall risk management program. Other factors such as location, specific vulnerabilities, and cost-benefit analyses can also be utilized to ensure a complete and comprehensive resilience picture for the asset.\(^4\) The assets specific resilience information, used in conjunction with information on the vulnerabilities and consequences can provide decisionmakers with a holistic risk picture in which to make management and policy decisions ensuring the continued protection and resilience of our nation’s critical infrastructure.

---

\(^3\) The data displayed for the facility is static, reflective of the relative resilience of the facility at the time of the survey

\(^4\) Facility vulnerability information can be ascertained via the PMI, and consequences via the consequence information collected in the survey