QinetiQ

CPNI
Centre for the Protection of National Infrastructure

Threat Image Projection (TIP) Guidance

Introduction

X-ray screening is a challenging role requiring rapid decisions on whether or not items are 'clear' or should be sent for further screening. The threats Security Officers are expected to detect vary in their materials, construction and shape, from Improvised Explosive Devices (IEDs) to handcuffs and padlocks used by protestors.

In many locations Security Officers could screen for their entire career without seeing a real threat, yet they need to remain vigilant, as every item they screen could contain a threat that could potentially result in loss of life if undetected.

Threat Image Projection (TIP) is a powerful tool designed to support the Security Officer in their task. It removes some of the tedium of the role by presenting the Security Officer with real threats within an X-ray image on a random, yet regular basis. It provides training by providing the Security Officer with images of threats that the organisation believe could be used against them and it identifies training needs by providing feedback on performance.

For organisations and managers, TIP provides data on where their greatest vulnerabilities are both in terms of location, vulnerable times and the threat most likely to be missed.

This document is designed to help Security Officers, their Supervisors, managers and the organisations that employ them to make the most of TIP systems and the data it provides. It is divided into seven sections.

- Understanding TIP
- The benefits of using TIP
- Implementing TIP
- Analysing TIP data
- Providing performance feedback to Security Officers
- Maintaining the value of TIP data
- Annexes providing further information

Throughout this document the term 'threat items' includes actual threats as well as other items of potential interest to an organisation (e.g. tools, disruptive items that may not pose a danger to life).

Understanding Threat Image Projection

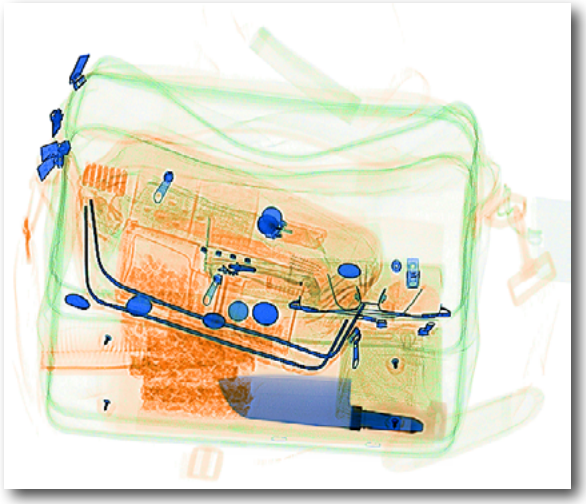
Threat Image Projection (TIP) is a software programme that inserts fictional (but realistic) images of actual threat items into the images of real items being screened using X-ray systems. TIP is available as standard software on most X-ray machines.

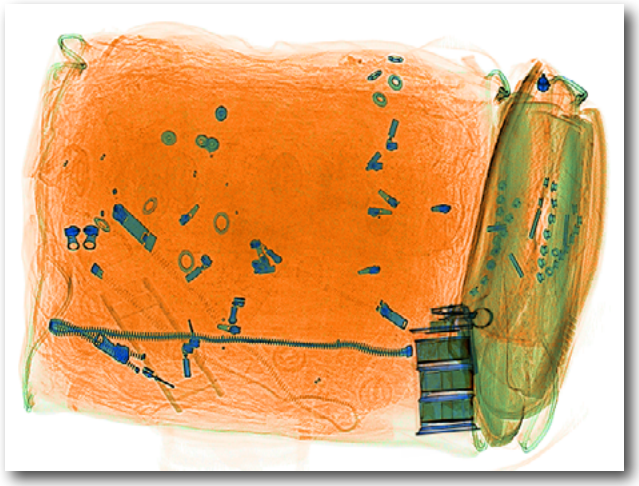
TIP is designed to enhance security through improving the threat detection performance of Security Officers by exposing them to artificial but realistic images of threat items during routine screening operations. For the Security Officer this can be a very useful motivational tool that helps to enhance their vigilance and exposes them to the sort of threats they are expected to recognise during their duties.

A Fictional Threat Item (FTI) appears as a real threat within the item being screened (e.g a bag, coat, mail). There are no cues available to the Security Officer to indicate whether the threat is real or fictional. The Security Officer's task, as with real threats, is to detect these FTIs when they appear.

The advantages of using FTIs are that they can be varied, are easy to develop, easy to project into the item being screened and each threat and item combination is unique. The FTI should be relevant and align to the organisation's needs and priorities (see Maintaining the Value of TIP data).

If the Security Officer identifies a threat they press the 'search' or 'reject' button on the control panel. On doing so, the Security Officer receives immediate feedback about the accuracy of their response. One of the following three, colour-coded feedback messages will be displayed. The messages are colour-coded to enable easy interpretation of the response and are shown on the following page.





Some examples of FTI projections

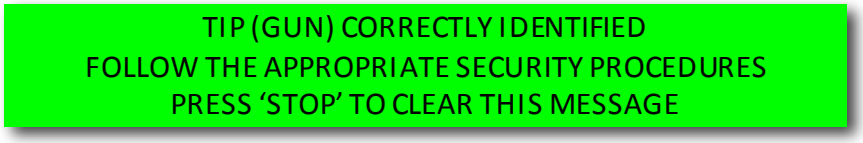
‘Hit’ Feedback Message

A ‘Hit’ message informs the Security Officer that they have correctly identified a FTI.

The message remains on screen until the STOP button is pressed. The message will instruct the Security Officer to re-examine the item for the presence of any real threats.

The location of the FTI will be shown and after a predetermined delay the FTI will be removed leaving the image of the item.

If the ‘search’ or ‘reject’ button is pressed after the TIP has been removed, a Non-TIP alarm message will be shown.



Example of a ‘Hit’ feedback message

‘Miss’ Feedback Message

A ‘Miss’ message informs the Security Officer that they have failed to identify a FTI.

The message remains on screen until the STOP button is pressed. The message will instruct the Security Officer to re-examine the item for the presence of any real threats.

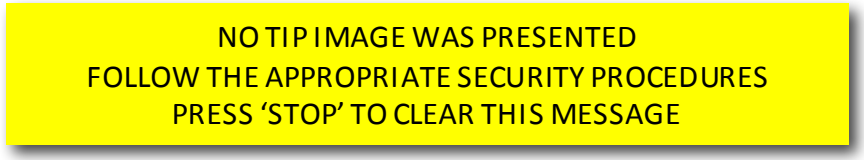
The location of the FTI will be shown and after a predetermined delay the FTI will be removed leaving the image of the item.

Example of a ‘Miss’ feedback message

‘Non-TIP Alarm’ Feedback Message

A non-TIP alarm informs the Security Officer that a FTI was not presented. Since the Security Officer believed that a possible threat was present, appropriate security procedures (i.e. a hand search) should be carried out.

This message remains on the screen until the STOP button has been pressed.



Example of a ‘Non-TIP’ feedback message as it appears on screen

‘Cancelled’ Feedback Message

The final message that the Security Officer might receive is the ‘cancelled’ feedback message. This message is presented if there is a system error inserting the FTI into the item and the image has been cancelled.

Example of a ‘Cancelled’ feedback message as it appears on screen

TIP Software

TIP software is contained within the X-ray machine system. It controls the projection and placement of the FTIs.

All activities that relate to the administration of TIP are undertaken via the TIP Management System (TMS) which is a sub-component of the TIP software. The TMS facilitates the management of TIP X-ray users viewing and downloading of TIP performance data and scheduling of TIP parameters. Only the TIP administrator, who is authorised to use the TMS, should have access to it.

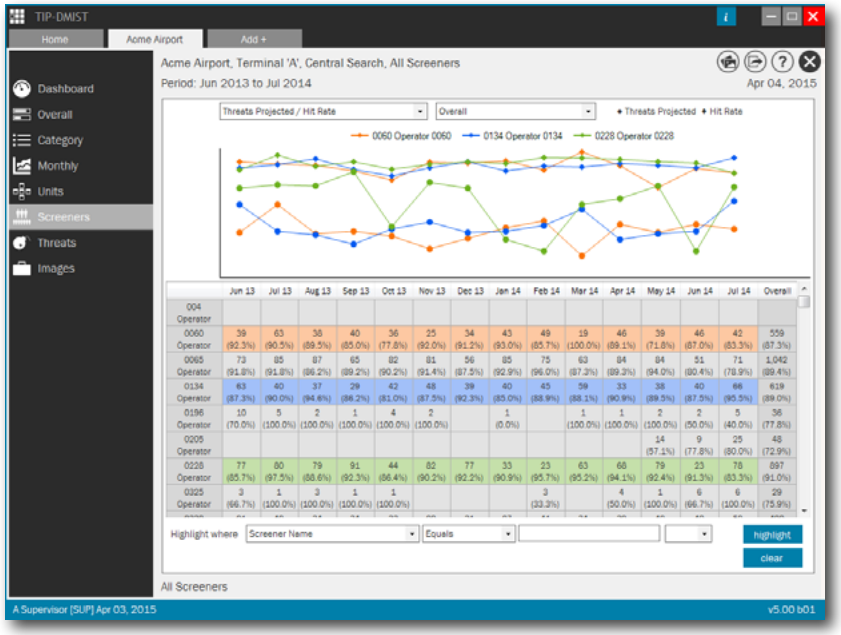
The benefits of using TIP

TIP is designed to enhance security by improving the threat detection performance of Security Officers.

In particular, there are six key benefits:

1. **Exposure to multiple threats over time**. TIP presents the Security Officer with a range of threat types, therefore increasing the Security Officer's knowledge base of what constitutes a threat. Familiarity with X-ray images of these FTIs helps to improve recognition ability for actual threat items when they occur. This is particularly useful for threat types that occur infrequently. New FTIs can be incorporated into the TIP image library at any time. This might be in response to a specific threat, evolving trends or simply to increase the variety of FTIs within the TIP library. This allows flexibility within the system.
2. **Security Officer motivation**. X-ray screeners enjoy using TIP. It maintains their motivation and interest in the screening task. Screeners are more motivated to do well by virtue of receiving regular performance feedback.
3. **Instant feedback**. Security Officers receive instant feedback on the decisions they make during the screening process so they are aware of their own performance.
4. **Security Officer vigilance**. FTIs provide the Security Officer with targets to detect thereby reducing the monotony and boredom that can be experienced with repetitive tasks that require sustained attention.
5. **Automatic generation of reports**. The TIP system generates five reports. These reports provide feedback on information that is beneficial for analysing risk, measuring performance, quality control and identifying training needs. This will alert the organisation to any weaknesses in the system.
6. **Flexible configuration**. A variety of TIP settings can be adjusted to meet the needs of the organisation. For example, the frequency of projection of FTIs can be set according to the throughput of the organisation, and to maintain Security Officer vigilance. The percentage of each category of threat can also be varied. This will ensure that Security Officers will get to experience a range of threats during their screening duties.

It is important to note that whilst the installation of TIP will no doubt enhance the screening process it should not replace other security processes and practices. For example, identifying a USB stick hidden within a book may require an additional screening process to find the threat, such as manual search.



This section explains how to introduce TIP gradually into the organisation so that its benefits can be fully understood. It explains the importance of assigning roles and responsibilities for TIP and considers the level of training that might be required.

Assignment of roles

It is recommended that at least one person (the Security Manager, Deputy Manager, Trainer or Supervisor) should be assigned the responsibility of managing the TIP system, known as the 'TIP Administrator'.

The TIP Administrator should determine who can access the system and at what level.

Suggested TIP responsibilities and access are shown in the table below:

Level	User	Roles
1	**TIP Administrator**	Set TIP ratios Select threat categories Access to TIP libraries Set and alter passwords Download data Maintain employee records View and print data reports Log on and log out
2	**Security Trainer**	Set and alter passwords Download data Maintain employee records View and print data reports Log on and log out
3	**Supervisor**	View and print data reports Log on and log out
4	**Security Officer**	View and print personal reports Log on and log out

Raising awareness of TIP

Security Officers will react differently to the introduction of TIP depending on their circumstances and understanding of the technology. Some Security Officers may have some concerns about the introduction of TIP. Security Officers who are both opposed to and in favour of the TIP system will need to be supported during the change process. It is important to explain to Security Officers that the main purpose of TIP is to optimise performance and provide feedback, rather than to be used as an enforcement tool.

The following six-step approach is recommended when introducing TIP:

1. Prepare a communication strategy.
2. Develop a set of Frequently Asked Questions (FAQs) for management to use when briefing security staff on TIP.
3. Inform key stakeholders on the rationale for using TIP within the security system.
4. Brief senior managers on TIP.
5. Conduct face-to-face briefings with Security Officers on TIP. These briefings should provide Security Officers with an understanding of the benefits of TIP and how it will impact their daily operations. Security Officers should all be briefed within a short space of time to reduce the likelihood of inaccurate information passing between staff. The briefing should also provide staff with some examples of the types of images included within the TIP library and how frequently they will appear to allay any concerns regarding difficulty and speed. Security Officers should also be briefed on the actions they need to take when they believe they have identified a potential threat (i.e. press the 'search' or 'reject' button). It is important that Security Officers are given the opportunity to ask questions and voice any concerns they have at this point. These briefing sessions should be well planned and are likely to take about 1.5 hours.
6. Prepare an internal briefing note that can be issued to all security staff providing them with an overview of TIP and the strategy behind its use.

Training

After the six-step approach has been completed, training for staff should also be provided. Training should be tailored to suit the audience. It is anticipated that each training session would take approximately 1.5 hours. See the table below for guidance.

Who	What
Training for Security Managers (any deputies), Trainers and Supervisors	Training on how to use the TIP Management System (TMS). How to interact with the X-ray unit whilst TIP is in operation.
Security Officer training	The use of the X-ray unit whilst TIP is in operation. NB. Security Officers should NOT be trained on the use of the TMS.

Training should be conducted away from live operations in an environment that allows the trainee to make mistakes in a 'safe environment' and to learn from them.

During training it is recommended that TIP-to-item[1] ratios should be set to 'High' so that Security Officers become familiar with how a FTI is presented within a item and the feedback messages.

Ideally FTIs used during training should not be employed during operations to prevent the Security Officer from identifying a threat simply because they recognise it.

Once all staff have received training on TIP, it is recommended that a one to three month period of operational familiarisation is undertaken. Initial analysis of the data gathered during the familiarisation period could be undertaken to check that the system is working. During this time period, Security Officers should be allowed to become familiar with the hardware/software and how the system is used during daily operations before performance data is analysed.

[1] TIP-to-item ratio is the number of items that have to be screened before a TIP is projected.

Where there is a risk of low acceptance of TIP by Security Officers, it is suggested that a generic rather than individual log-on is used for the first one to three months followed by the introduction of individual logons after the initial familiarisation period.

Individual logons

It is recommended that unique log-on IDs and passwords should be assigned to all Security Officers. This will allow the organisation to monitor use of the machine and gather data which can be used to support training. All responses made by an individual Security Officer can be collated allowing a picture of individual strengths and weaknesses to be built up over time. This will provide a rich picture of the Security Officer's performance allowing the Supervisor to provide feedback and tailor training as necessary.

If a Security Officer is logging on to more than one machine the same log-on ID and password should be used.

When a Security Officer logs on a feedback message containing their name is presented to confirm that they have logged on correctly.

The log on procedure takes less than 10 seconds and the log off procedure is equally quick and simple.

All passwords should be treated as confidential and should not be shared with other staff or written down.

TIP Scheduling

A scheduling system is present on the TMS to ensure that Security Officers cannot predict when a TIP will be projected. There are three key parameters that need to be considered:

- **TIP-to-item ratio** (the number of items that have to be screened before a FTI is projected). It is recommended that the TIP-to-item ratio should be set to a level of 1:50 for locations with a high throughput and 1:35 for locations with a lower throughput . The ratio should be set so that it will result in 1-2 FTI projections every 20 minutes (if there is a constant throughput of items).
- **Item range** (the variation between the lowest and highest values). The item range should be variable from 0% to 100% based on the TIP-to-item ratio. For example, if the TIP-to-item ratio is one TIP in every 50 items and the item range is set to 10% a TIP should randomly appear within a range of 45 to 55 items. This is to stop Security Officers being able to predict exactly when a FTI will be projected.
- **Random ratio** should be variable from 0% to 50% allowing a proportion of the FTIs to occur randomly within the TIP-to-item ratio limit.

In addition:

The percentage at which each threat category of FTI is presented can also be specified (e.g. Knives = 25%, Guns = 25%, IEDs = 25%, Electronics = 15%, Disruptive items = 10%). This allows organisations to adjust the category percentages to reflect their threat priorities.

The initial decision time (the time period for which the FTI stays on the screen before the system 'times out' and classifies the FTI as a Miss) can be varied from between five and seven seconds.

The secondary decision time (when the screening process has stopped and the Security Officer can conduct further analysis before making a response) can be varied from between ten and thirty seconds.

To explain how the three TIP scheduling settings work together an example is provided below:

If the TIP-to-item ratio was set at one TIP every 50 items and the other two settings were set to zero, then, TIPs will be evenly spaced and predictable.

Scheduling using just the TIP-to-Item ratio, TIPs are evenly spaced and predictable.

In addition to setting TIP-to-item ratio, if the item range is set to 10%, then a TIP will be presented between every 45th and 55th item (as indicated by the green bars in the diagram below).

Scheduling using TIP-to-Item ratio and item range, TIPs are not evenly spaced but still predictable.

The final setting, the random ratio, is used to remove this predictability. If the random ratio is set to 10%, then 90% of the TIPs would appear between every 45th and 55th item. The other 10% of TIPs would appear 'randomly' at any point during the screening process (as indicated by the orange bar in the diagram below). By using all three settings it is possible that two TIPs could appear in consecutive items (as indicated by the overlap of the green and orange bars).

Scheduling using all three settings, TIPs are not evenly spaced and not entirely predictable.

Analysing TIP data

This section explains how to analyse TIP performance data. It details what data is captured and how to access this data by producing one of five TIP reports. Factors that could impact on TIP performance are also discussed. A step-by-step guide to analysing data from single and multiple machines can be found in Annex A.

Data captured

TIP systems have the capacity to record a wealth of data. The data can be analysed to obtain various measures of organisational and Security Officer performance.

Specifically, TIP records the following data categories:

- Time logged on and off.
- Number of shifts worked.
- Number of items screened.
- Number of Hits and Misses (by threat item).
- Number of Non-TIP alarms.
- Hit rate.
- Non-TIP alarm rate.
- d' (d prime) (d' is a measure of screener threat detection performance that takes into account the number of Hits and Non-TIP alarms).
- Reaction time for Hits.
- Reaction time for Non-TIP alarms.
- Decision outcome (Hit, Miss, Non-TIP alarm and correct rejections).

Each month, five TIP reports are automatically generated (see Annex B).

TIP Report 1 (Screener Log) - contains information about which screeners logged into the TIP system each day and their log in and out times.

TIP Report 2 (Individual Screener Performance Summary) - contains screeners' *daily* performance data for a given month.

TIP Report 3 (Screener Comparisons) - contains performance information for all screeners over a given month.

TIP Report 4 (Threat Detection by Category) - contains information on the specific threat images presented to each screener, together with the associated decisions made.

TIP Report 5 (Change to settings) - contains information about changes made to settings, when and who by.

Data preparation

Data can be downloaded from the X-ray system at any time although it is suggested that data should be downloaded once a month. Once the data has been downloaded it is recommended that the data files are copied onto a computer and a back-up is made. The raw data should not be deleted from the machine until a back-up copy has been produced.

When downloaded, the reports are in a text file format. The filename indicates which machine the data are from, the time period the data covers and the type of report.

It is recommended that trend data gathered over a minimum of four months with at least 80 FTI presentations are used in the analysis. If less than 80 FTIs have been presented during a four month period this period will need to be extended until at least 80 FTIs have been seen. Conversely, if a Security Officer views 80 FTIs in under four months analysis of the data must not be conducted until the full four month time period has elapsed. Analysing less than 80 FTIs and four months' worth of Security Officer data is insufficient and could lead to inaccurate or unfair decisions being made about a Security Officer's performance.

Whilst out of scope of this guidance document, the security and the sensitivities surrounding the data downloaded in the TIP reports should be considered and the information handled in an appropriate manner.

Analysis

For a step-by-step guide to analysing data from single or multiple machines please refer to Annex A.

More advanced analysis can be conducted to better understand a Security Officer's ability to identify threats. Specialist software is available to simplify the data analysis process or to enable more advanced analysis to be conducted (an example of this can be found at Annex C).

Factors that could impact on TIP Performance

It is important to note that performance statistics can be influenced by a number of key factors. These factors must be taken into account to enable a fair and accurate assessment of Security Officer performance to be made.

1. **Number of FTIs projected**. When analysing performance, actual numbers of FTIs 'hit' and 'missed' must be considered in addition to percentages. A greater number of projected FTIs give a more accurate picture of Security Officer performance. Fewer FTIs leads to more extreme percentage scores, as shown by the table below.

No. of FTIs Projected	No. of Hits	Hit Rate	Difference
3	3	100%	25%
4	3	75%	
30	27	90%	3%
31	27	87%	

Where throughput is low, a higher TIP-to-item ratio should be considered.

2. **Difficulty of the FTIs Projected**. The TIP library will contain FTIs of varying difficulty, i.e. one knife may be easier to detect than another. Difficulty also varies according to the angle at which the FTI is presented. For example, a gun may be easy to detect when presented side-on but difficult to detect from above. It is not possible to ensure that all Security Officers see FTIs of equal difficulty. To ensure a fairer, valid and reliable assessment of Security Officer performance, a minimum number of FTIs must be included in any performance analysis to mediate the effects of variation in difficulty. It is recommended that a minimum sample of 80 FTI projections is used to provide an indication of Security Officer performance (see Annex D).

3. **Complexity of the item image and superposition**. Each item that is screened differs in its content and as a consequence, the ease with which an FTI can be detected. For example, it may be more difficult to detect a gun FTI in an item full of other metal items compared with an item containing mainly organic items. Superposition, when items are superimposed on one another, can also increase the difficulty of detecting the FTI. To mitigate this, it is suggested that a minimum number of items screened (at least 80 FTIs) are used in the analysis of Security Officer performance. Any variation in performance caused by item complexity/superposition will reduce across a large data set (see Annex D).

Providing performance feedback to Security Officers and assessing organisational performance

This section provides guidance to Supervisors and Security Managers on how TIP data can be used to provide performance feedback at an individual level (to Security Officers), at a group level and also the benefits from an organisational perspective. Such analysis helps organisations recognise the strengths and weaknesses in their security and why performance on certain threat items is lower than others.

TIP Reports '2' and '4' are the most useful for conducting Security Officer performance analysis.

Individual performance data

It is possible to assess the individual strengths and developmental needs of individual Security Officers using TIP data. For example, TIP data can reveal the threats that Security Officers are most likely to detect as well as those items that they are consistently missing. Training interventions can then be devised that concentrate on improving detection performance for those items. By analysing trend data, it becomes possible to monitor a Security Officer's performance over time and to identify whether any training interventions are having an impact.

TIP performance results can be fed back to Security Officers. Studies have found that the provision of feedback, in the form of performance statistics and those images a screener has missed, improves threat detection performance.

TIP data can provide a useful measure of job performance. However, it must be used and interpreted in the correct way to ensure fairness and reliability. Conclusions about a Security Officer's performance should be made only when sufficient data have been collated and analysed and when the reliability of individual TIP performance indicators has been demonstrated. It is recommended that analysis is only conducted when a Security Officer has seen at least 80 FTIs.

Group performance data

It is possible to determine detection rates for groups of Security Officers and to use this information to motivate individuals to work as a team by offering incentives/rewards to the best performing groups. By encouraging collective responsibility for improving TIP statistics, it is possible to positively impact the performance of individuals. For example, the data can be used to identify why group performance for particular threat categories is low and to adjust training needs.

Organisational level data

Establishing performance baselines for Security Officers across comparable organisations provides insights into the types of threats that are being detected and those that are being missed. This information can be used to implement more effective TIP image library management. See next page 'Maintaining the value of TIP data'.

Maintaining the value of TIP data

To preserve the value of TIP data, the library of TIP images should be regularly maintained and updated. This section explains why this is important, how this task should be undertaken, and how frequently.

The TIP image library is the repository for all FTIs.

Maintaining the content of the TIP image library is important because it ensures that an appropriate threat detection challenge is presented to Security Officers, enhances the acquisition of threat knowledge amongst Security Officers and as a consequence may increase the accuracy of the threat assessment made. As a minimum there should be 1,000 TIP images in the library when it is first installed.

The TIP image library should comprise a number of categories, for example:

- Guns
- Knives
- IEDs
- Disruptive Items (i.e. padlocks and handcuffs)
- Tools
- Weapons

TIP also offers the option to increase the number of threat categories over time.

All TIP images must be realistic. It must not be possible to distinguish between a real threat and a TIP item. The image library should contain images of the same threat at different orientations. To avoid high abort rates, TIP items should be selected so that they can be projected into scanned items without the system having to abort the insertion.

It must be possible to cross-reference these as the same threat by ensuring that each image has a unique and meaningful filename. This information can then be used to assess (by running TIP report 4) whether a particular FTI is easier/harder to identify from a particular orientation. Further action (such as additional training) may then be required.

Repeated exposure to the same TIP images will allow Security Officers to learn what the FTIs in the image library look like. Whilst it is desirable for Security Officers to learn the features of threat items it is not desirable for Security Officers to be able to recognise specific FTIs within the image library.

How frequently the library should be updated will depend on the:

- Size of the library
- TIP parameter settings (TIP-to-item and threat projection ratios)
- Difficulty of the images
- Amount of time a Security Officer spends screening
- Organisational throughput
- When threat and organisational priorities change

It is recommended that images should be updated after they have been projected four or five times to the majority of Security Officers to prevent them from becoming familiar with the images.

Managing the TIP library

Using a bespoke TIP library rather than the library provided by the manufacturer will ensure that the FTIs used are appropriately aligned to the organisations needs and priorities

TIP image libraries can be managed in two ways:

1. **Use a small library, which is frequently changed**. Old images are removed and new images are added. Assessing which items are detected frequently, occasionally and never will aid decision making about the items that need to be removed and the types of image that should be present.
2. **Use a large and representative library**. Growing the library so that there are a vast array of images that can be used and removing items on an annual basis to prevent Security Officers becoming familiar with the library.

Single Machine Analysis

Below is a step-by-step guide to conducting performance analyses using TIP Report 2 after the data has been downloaded from one machine.

TIP Report 2: Basic performance statistics

Step 1: Open the text file into a spreadsheet package. The report will show one row of performance data for each Security Officer for the time period covered.

Step 2: Calculate totals for Items Screened, FTIs Projected, Hits, Non-TIP alarms, and Misses by summing the data for all Security Officers shown in the report.

Step 3: Obtain basic performance statistics using the calculation functions within the spreadsheet package. For example:

$$\text{TIP-to-item ratio} = \frac{\text{Total number of Items Screened}}{\text{Total number of TIPs Projected}}$$

$$\text{\% Hits} = \frac{\text{Total number of Hits}}{\text{Total number of TIPs Projected}} \times 100$$

$$\text{\% Misses} = \frac{\text{Total number of Misses}}{\text{Total number of TIPs Projected}} \times 100$$

Steps 2 and 3 can also be used to calculate performance statistics for specific groups of Security Officers, such as new starters.

TIP Report 4: Performance statistics by threat category (e.g. guns or knives)

Step 1: Open the text file in a spreadsheet package. Each data row represents an occasion where a Security Officer pressed 'search'.

Step 2: Use a filter function to sort the data into threat categories. Select a threat category type to specify those occasions where that type was projected; note the number of threats selected when using this filter.

Step 3: Whilst the filter in Step 2 is applied, select 'hits' or 'misses' under the decision outcome column. This will select all the occasions in which a particular type of FTI was 'hit'/'missed' by the Security Officer. Note the number of cases selected using this filter.

Step 4: Repeat Steps 2 and 3 for the remaining categories.

The following performance statistics can then be calculated:

$$\text{\% Hits [e.g. knives]} = \frac{\text{Total number of Hits [e.g. knives]}}{\text{Total number of TIPs [e.g. knives]}} \times 100$$

$$\text{\% Misses [e.g. knives]} = \frac{\text{Total number of Misses [e.g. knives]}}{\text{Total number of TIPs [e.g. knives]}} \times 100$$

To calculate these performance statistics for individuals or groups of Security Officers, records that relate only to those Security Officers must be accumulated, using a filter function on the 'name' column. To create groups of Security Officers, add an additional column, label the group appropriately and then filter according to the required group.

TIP Report 4: Analysing missed image data

Step 1: Open the text file in a spreadsheet package. Each data row represents one occasion where a Security Officer pressed 'search'.

Step 2: Using a filter function, select a FTI filename from the list presented under the FTI Projected column to specify only those occasions where the individual threat was projected and note the number of cases. Perform this step for each threat to be investigated.

Step 3: Using a filter or sort function, select 'hits' or 'misses' under the decision outcome column. This will select only those occasions where a Security Officer 'hit'/'missed' a projected FTI.

Step 4: Using a filter or sort function, select a threat filename from the list presented under the FTI Projected Column to specify those occasions where a screener 'missed' that particular threat and note the number of cases. Perform this step for each threat to be investigated.

Step 5: Calculate the percentage of times each threat was hit and missed using the following calculation:

$$\%\ \text{Hits [FTI 'A']} = \frac{\text{Total number of FTI 'A' Hits}}{\text{Total number of FTI 'A' TIPs}} \times 100$$

$$\%\ \text{Misses [FTI 'A']} = \frac{\text{Total number of FTI 'A' Misses}}{\text{Total number of FTI 'A' TIPs}} \times 100$$

Once the most frequently missed FTIs are identified it may be useful to obtain pictures of these threats from the library of images stored on the X-ray machine. Trends within these images may then emerge to suggest why Security Officers are missing these items.

Multiple machine analysis

If a Security Officer has logged-on to more than one machine in any given month it will be necessary to download data from all of these machines to gain a full picture of that Security Officer's performance.

When data from more than one X-ray machine needs to be analysed, greater workload demands are placed on the analyst because of the large number of reports to analyse. It is recommended that more sophisticated TIP data analysis tools (e.g. TIP-DMIST™) are used for this purpose. These tools can automate the data verification, sorting, storage and analysis thereby substantially reducing the effort required by the analyst.

When analysing data from multiple machines, the following procedure should be followed:

- All TIP Reports '2' and TIP Reports '4' downloaded in a month should be combined, either manually (using the copy/paste function), or using a macro procedure. All data from TIP Reports '2' should be in one data file (Combined 2) and all TIP Reports '4' should be in another file (Combined 4).
- For the Combined 2 file, records for each individual Security Officer need to be aggregated. If a Security Officer has logged onto three X-ray machines in one month, for example, the three rows of data must be summed together to obtain one row of performance data. An average (mean) score based on overall performance on each machine is not sufficient.
- For the Combined 4 file, entries for each individual Security Officer must be combined. For each Security Officer, records should be grouped by threat type and by response.
- The above calculations can be automated using formulas.

Annex B The contents of the five TIP reports

The following table details the contents for each of the five TIP Reports.

Field	TIP Report 1 (Screener Log)	TIP Report 2 (Individual Screener Performance)	TIP Report 3 (Monthly Screener Comparison)	TIP Report 4 (Threat Detection by Category)	TIP Report 5 (System Log)
1	Name	Name	Name	Name	Name
2	ID number	ID number	ID number	ID number	ID number
3	Company	Date	Number of items screened	Date	Date
4	Location	Number of items screened	Number of FTIs presented	Time	Time
5	Machine type	Number of FTIs presented	Number of Hits	FTI projected	Changes made to settings
6	Machine serial number	Number of Hits	Number of Non-TIP alarms	Threat category	
7	Log on time	Number of Non-TIP alarms	Number of Misses	Threat sub-category	
8	Log out time	Number of Misses	Probability of a Hit	Decision outcome	
9	Date	Probability of a Hit	Probability of a Non-TIP alarm	Response time	
10		Probability of a Non-TIP alarm	d’		
11		d’	Decision time for a Hit		
12		Decision time for a Hit	Decision time for a Non-TIP alarm		
13		Decision time for a Non-TIP alarm	Number of logins		
14		TIP-to-item Ratio			
15		Variance / Diversification range			
16		Random Ratio / Random Projections			

Annex C Using TIP-DMIST™ to conduct more advanced analysis

The TIP Data Management and Interpretation Software Tool (TIP-DMIST™) has been developed by QinetiQ, and is the only product that can analyse TIP data from multiple manufacturers by converting TIP data into an easily useable form. It is based on over 15 years of working with Government departments, operators and security providers. TIP-DMIST™ supports the collection, assimilation and data cleansing of TIP data from a multi-vendor environment within a secure storage environment.

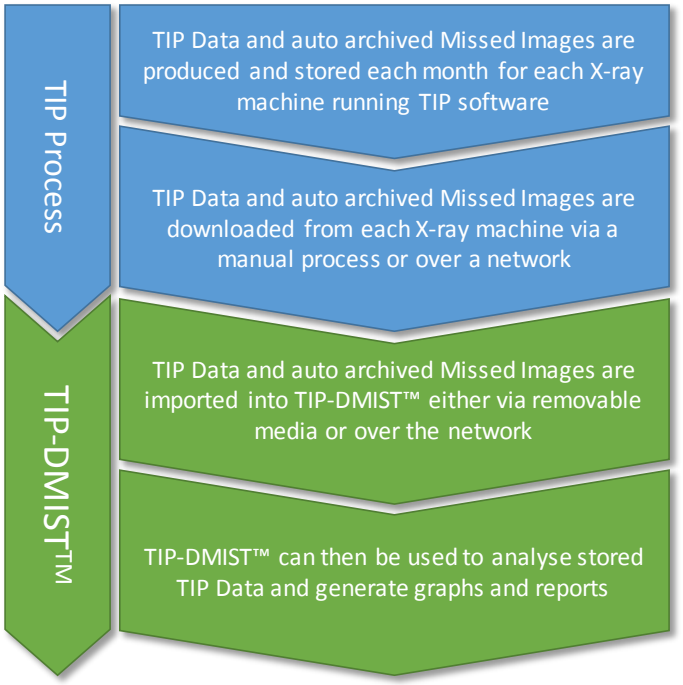
TIP-DMIST™:

- Enables organisations to make better informed decisions about individual, team and overall performance.
- Provides evidence as to whether the workforce is achieving highest standards of security screening.
- Provides evidence as to the effectiveness of selection and training.
- Identifies gaps in performance.
- Allows instant communication of meaningful threat detection performance information.
- Provides a user friendly interface suitable for use across all levels of staff, including Directors, Security Managers, Security Trainers, Supervisors and Screeners.
- Cost savings in relation to time and resources spent on analysing and managing TIP data.
- Provides an audit trail for screener performance in light of changes to security procedures.

TIP-DMIST™ has the following broad capabilities:

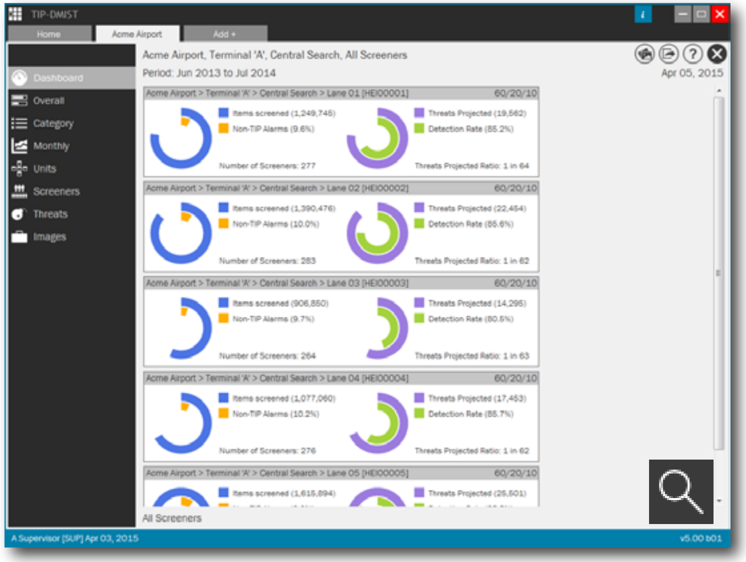
- Secure storage and effective management of TIP data.
- Selection of a wide range of performance criteria.
- Rapid analysis of TIP data to provide accurate, meaningful measurement of performance.
- Ability to view missed images and sort by threat category, date and screeners.
- Ability to compare data between search areas, X-ray machines, screeners or groups of screeners.

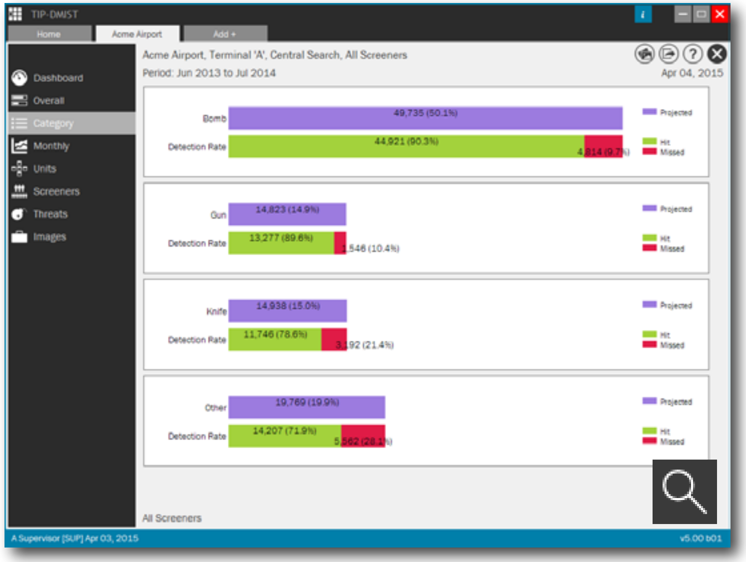
TIP-DMIST™ integrates with general TIP processes as follows:

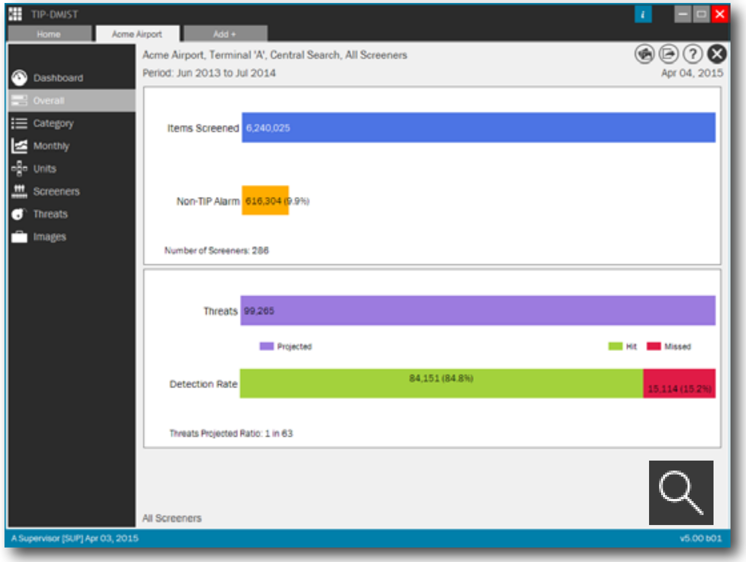


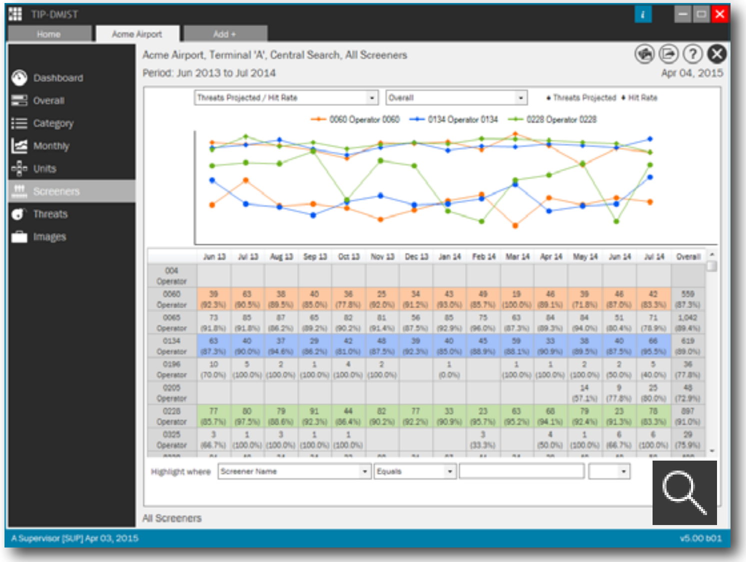
TIP-DMIST™

Data is presented graphically to make it easy to use including a Dashboard display, Overall Performance, Threat Category and Monthly Comparisons.





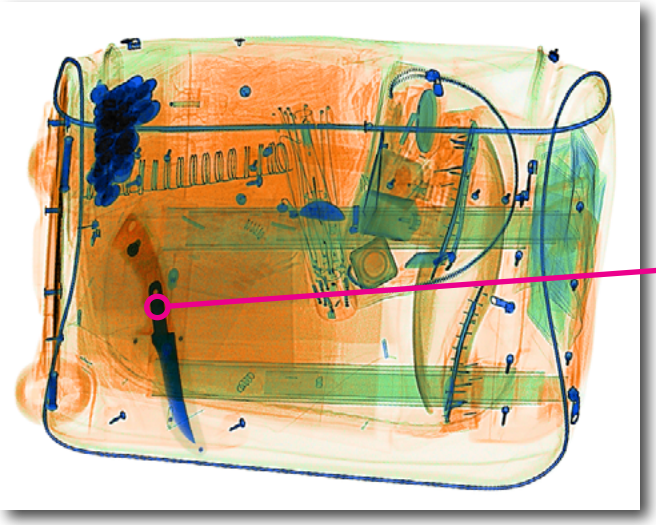




Examples of difficulty and superposition of images

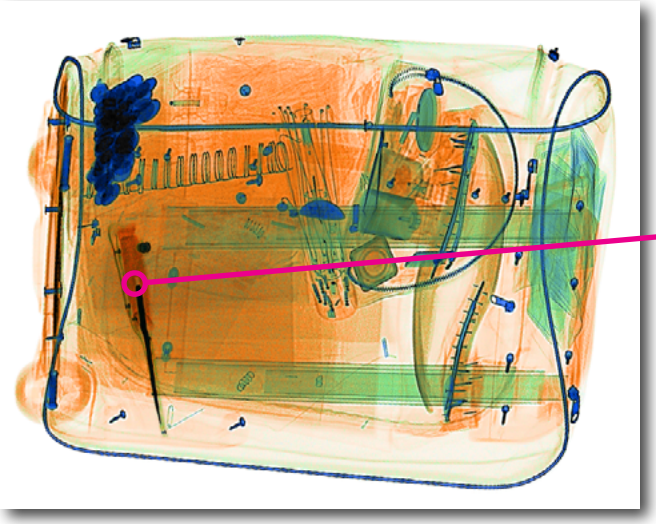
The combination of the complexity of the item, the placement of the FTI and its orientation can have an effect on detection.

The images below are of the same easy-to-medium complexity item. The four images show the same FTI of a knife, projected into different areas of the item, and at different orientations.

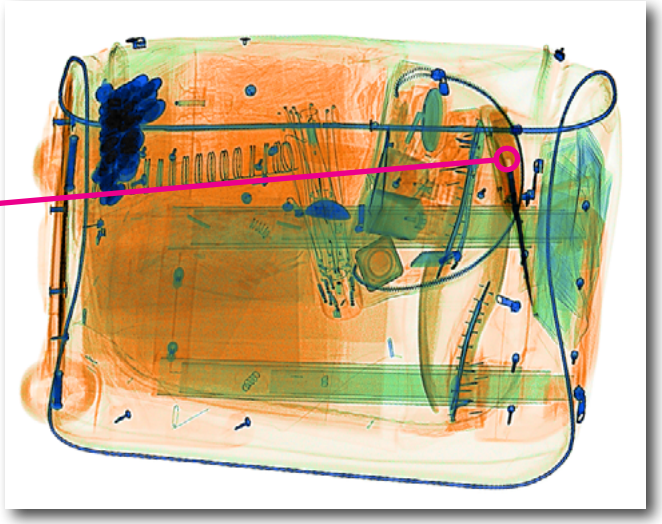


FTI projected into a less 'busy' area of the item

FTI projected into a 'busy' area of the item



FTI projected into less 'busy' area of the item but in a different orientation



FTI projected into 'busy' area of the item but in a different orientation

This page has intentionally been left blank.