HOME OFFICE JANUARY 2026

IRS PLUS G-CLOUD 15 SERVICE DEFINITION

MOTOROLA SOLUTIONS

The design, technical, and cost information furnished with this proposal is proprietary information of Motorola Solutions, Inc. (Motorola). Such information is submitted with the restriction that it is to be used only for the evaluation of the proposal, and is not to be disclosed publicly or in any manner to anyone other than those required to evaluate the proposal, without the express written permission of Motorola Solutions, Inc.

MOTOROLA, MOTO, MOTOROLA SOLUTIONS, and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2026 Motorola Solutions, Inc. All rights reserved.

Ref: 4225995, Issue 0

TABLE OF CONTENTS

1 IRS PLUS SERVICE DEFINITION 4
1.1 Overview 4
1.2 IRS Plus Systems Provided 4
1.3 Features Overview 4
1.3.1 Workflow and Validation 6
1.3.2 GIS 7
1.3.3 Direct SQL Reporting Access (Read Only) 7
1.3.4 Auditing 8
1.3.5 API (Application Programming Interface) 8
1.4 System Load Capacity and Scalability 9
2 IRS PLUS SERVICE SYSTEM DESIGN 10
2.1 FRS Access / Networking 13
2.2 Server Organisation 13
2.2.1 Application Server 13
2.2.2 Database Server 13
2.3 Customer Installed Components 13
2.3.1 CAD Interface 13
2.3.2 Web Browser 14
2.4 Security and Resilience 14
2.4.1 Web Traffic / Data in Transit 14
2.4.2 Firewall 14
2.4.3 User Authentication 14
2.4.4 Network / Internet Security 14
2.4.5 Monitoring 15
2.4.6 Data Segregation and Data Access 15
2.4.7 Data Storage 15
2.4.8 Asset Protection and Resilience 16
3 CUSTOMER SYSTEM ROLL-OUT (ON-BOARDING) 17
3.1 Common Elements 17
3.1.1 Training Courses 17
3.1.2 Documentation Provided 17
3.1.3 User and Access Configuration 17
3.2 Roll-out Process – Option 1: Single customer at a time 18
3.2.1 Training for Roll-out Option 1 18

3.2.2 Option 1 Roll-out Capacity 19
3.3 Roll-out Process – Option 2: Multiple customers at a time 19
3.3.1 Option 2 Roll-out Capacity 20
3.4 Roll-out Assumptions 21
4 SUPPORT 22
4.1 Question and Validation Rules Changes 22
4.1.1 Home Office Changes 22
4.1.2 FRS Changes 22
4.2 Software Releases 23
4.2.1 Software Testing 23
4.3 Web Browser Compatibility 23
4.4 Support SLAs 23
4.4.1 Target Responses 24
4.4.2 Priority Categories 24
4.4.3 Definitions 24
4.4.4 Scheduled Maintenance 24
4.4.5 Unscheduled Maintenance 24
4.4.6 Service Availability 25
4.5 Resilience 25
4.6 Exclusions 25
5 PRICING 26
5.1 IRS Plus Annual Prices 26
5.2 Microsoft Licensing 26
5.3 OS On-Demand and OS AddressBase Premium 26
5.4 General Caveats 26

1 IRS PLUS SERVICE DEFINITION

1.1 OVERVIEW

The IRS Plus system allows collection and analysis of post-incident information for Fire and Rescue Services.

IRS Plus is an alternative to the Home Office IRS system, allowing Fire and Rescue Services to capture incident information from their Command and Control System; augment it with additional information from crews, validate it, and transmit it to the Home Office's Web Service - thereby meeting their incident reporting obligations.

The IRS Plus System is provided as a Software as a Service (SaaS) cloud hosted system, and is used by a significant number of Fire and Rescue Services.

IRS Plus is provided pre-configured with the current Home Office (HO) questions and validation rules and thereby provides a drop-in alternative for the HO IRS system. If required, the questions and validation rules can be tailored to meet additional data capture requirements of customers.

1.2 IRS PLUS SYSTEMS PROVIDED

Each FRS is provided with a Live and a Test environment (costed option).

The Live environment allows end-to-end processing of incidents from the CAD system incident feed through incident form completion and validation and ultimately HO submission.

The Test system allows limited processing of incidents, including a feed from the CAD system (if available), incident form completion and validation. It does not include submission to the HO system. The Test system is also intended to be used for training purposes and for trialling software before it is released to the live system (e.g. preview of new functionality or configuration changes).

1.3 FEATURES OVERVIEW

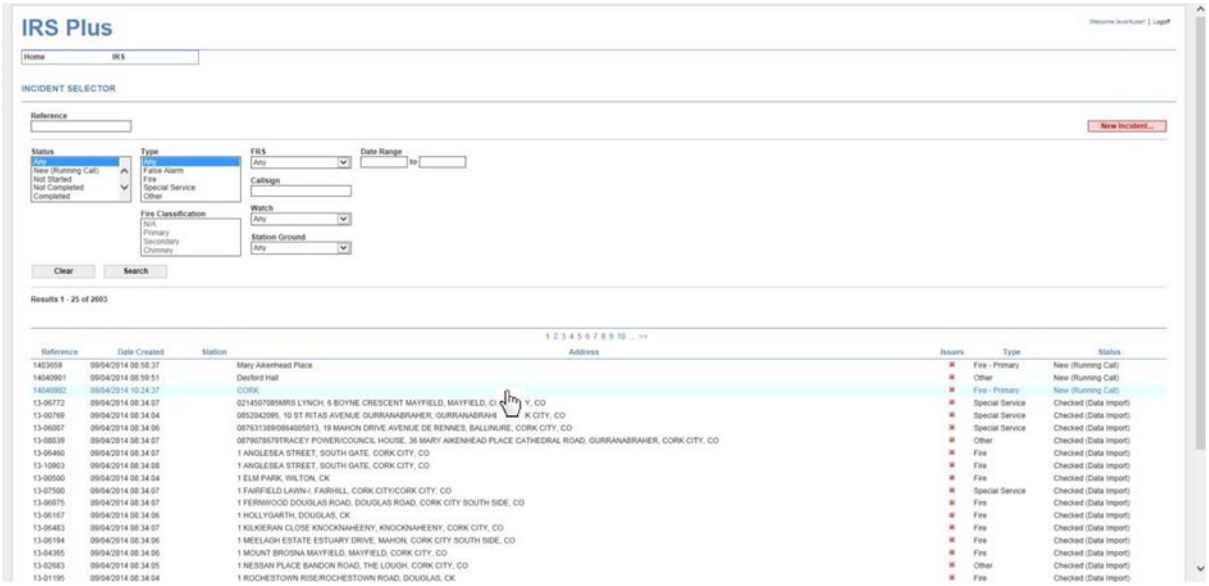
The core of IRS Plus is a web application that enables users to enter further details about incidents to supplement the data captured by their CAD system, and in certain circumstances to create "standalone" incidents.

The nature of the extra details requested by the application varies according to the requirements of each FRS, but may include such information as BA wearers, casualties, whether a fire investigation was carried out and by whom, medical assistance provided, and so on.

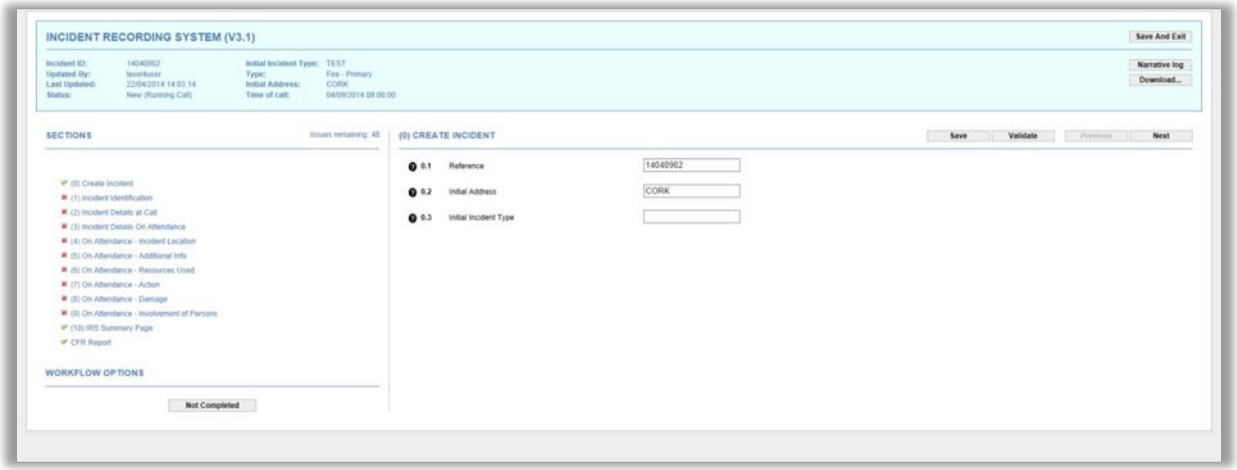
Data added via the application, together with data recorded by the CAD system is necessary for compiling statistical information for an FRS's own use and for National Statistics.

The main areas that make up the IRS Plus web application are:

- **Incident Selection** – perform a search for incidents that require completing



- **Incident Form** – complete the incident with the required details



- **Incident Reports** – access standard and ad-hoc reports
- **Create New Incident** – create stand-alone incidents
- **HO Uploads** – send completed and checked incidents to the Home Office (supported for UK FRSs only)
- **Security Manager** – manage security profiles within the application (administrative users only).

The Incident Forms and Incident Reports are built on a configurable framework which allows customers to add new questions, move or modify existing questions and otherwise customise the content of the IRS Plus system.

1.3.1 WORKFLOW AND VALIDATION

1.3.1.1 WORKFLOW

Incidents in IRS Plus follow a lifecycle defined by a configurable workflow. The standard configuration is built around four statuses:

- **Not Started** – the initial status of a new incident populated by the CAD system feed
- **Not Completed** – the incident is being edited and is awaiting completion
- **Completed** – the incident has been completed by the officer responsible, has no outstanding issues and is awaiting QA checks
- **Checked** – QA checks have been completed and the incident is ready to upload to the HO.

The IRS Plus workflow supports a flexible configuration which integrates with the security profiles to manage a user's ability to navigate an incident through the workflow.

New workflow stages can be added to support custom scenarios, such as sections which must be completed before or after the main content has been filled in.

1.3.1.2 VALIDATION

IRS Plus uses an incident report validation framework. The standard form configuration implements the HO IRS validation rules. Customers can define additional constraints for HO questions, as long as they are compatible with the HO's own rules.

Custom questions are treated as just another question by the validation framework, so the same kind of rules can be applied.

The validation framework can also be used to implement default answers and manage dependencies between questions; for example, filtering a list of stations by the FRS selected in a previous question.

Questions and sections can be enabled and disabled, shown and hidden, using rules based on the validation framework. This means that only those questions and sections in the IRS Plus form that are relevant are shown, simplifying the completion of the form.

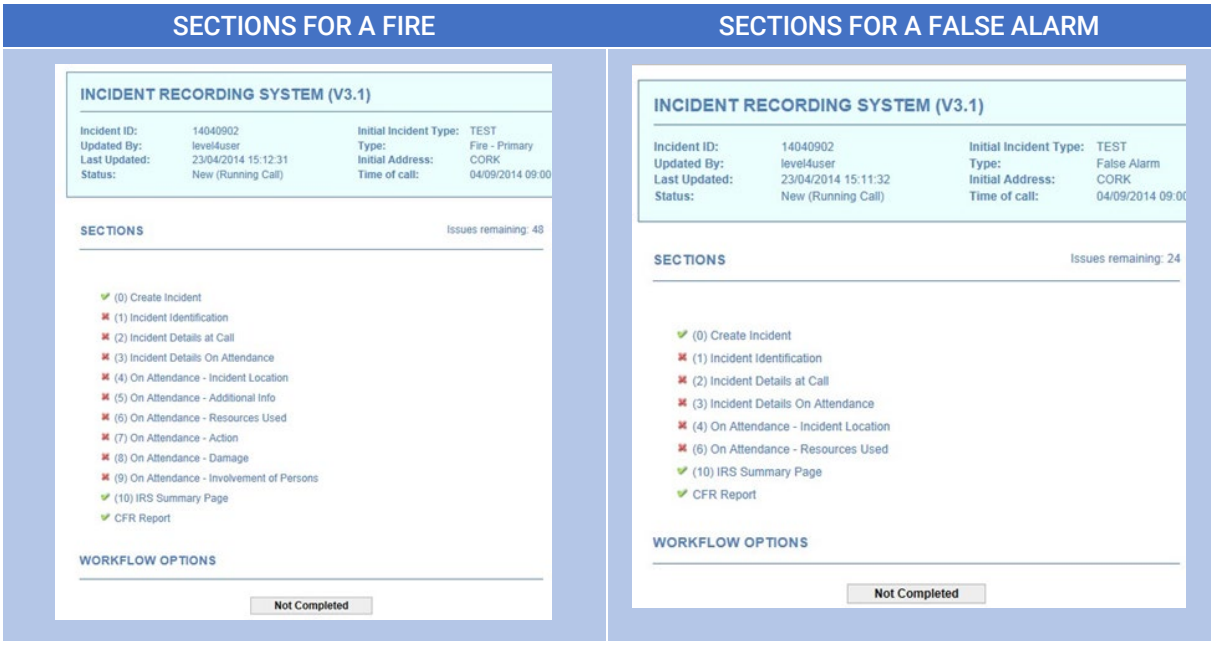


FIGURE 1 - EXAMPLE OF DIFFERENT SECTIONS SHOWN FOR DIFFERENT INCIDENT TYPES

The validation framework can be linked into the workflow system, allowing changes in the workflow stage to be controlled by the outcome of validating an incident. For example, in the standard configuration of IRS Plus, users cannot change the status to 'Completed' until all of the validation rules for an incident pass.

1.3.2 GIS

1.3.2.1 MAPPING

We provide the ability to integrate to an on-premise or cloud hosted CadCorp mapping system.

We have worked closely with CadCorp to provide a reliable integration to their Mapping API providing further functionality for increased incident reporting accuracy.

Supported functionality:

- The user can view the incident on a map (close to full screen). This allows panning and zooming of the map.
- The user can geo-locate the incident. They are able to move the incident location by selecting another location on the map. The new location is then stored in the IRS Plus system as the incident location.
- Any changes made to the incident location are audited.

1.3.2.2 GEO-CODING

IRS Plus provides integrated geo-location (gazetteer address lookup) for geo-verification of incidents. It also allows the incident to be tagged with a UPRN (if this is in the source data set).

Geo-verification of incidents adds huge value to IRS Plus incidents by allowing linking to other corporate information, such as Fire Safety, Risk Information, Premise Information and Fire Investigation.

The module allows users to search for addresses and select the incident location from a list of matching or partially matching addresses; the initial address will default to that provided by the CAD system.

The system supports uploading checked incidents to the HO's web service, allowing FRSs to fulfil their obligations for reporting incident data to the HO.

When the incident QA process is complete, they are available to be selected for uploading to the HO. Incidents can be uploaded individually or in batches.

Any validation errors reported by the HO system are recorded in the incident audit log so they can be corrected, and the incident re-submitted.

Incidents can be re-sent at any time. If an incident report is updated, for example following a fire investigation, once checked it can be uploaded again to amend the data recorded in the HO system.

1.3.3 DIRECT SQL REPORTING ACCESS (READ ONLY)

3tc provide direct SQL access to a separate reporting replica database, also hosted in Azure should this be required (at additional cost). The access provided can be accessed using SSMS either as a linked server, or as a direct connection to the database engine hosted in the cloud.

Splitting the DB hosting out into two separate instances, allows heavy-weight scripted reporting, without affecting the performance of the live application, without the need of downloading or backing up a database. This gives you 'up to the second' access to your data.

1.3.4 AUDITING

The IRS Plus system records an audit trail of data changes and significant events, including:

- An answer to a question is changed
- The workflow status of an incident is changed
- An incident is uploaded to the HO.

Audit events include a timestamp indicating the date and time of the event, the identity of the user or system that caused the event to occur and details of the specific event; for example, when data is changed in the system, the old and new values are recorded.

The audit log is available to view within the IRS Plus application. Access is controlled by security permissions, allowing users to restrict who can access audit logs.

When auditing starts is configurable within the IRS Plus workflow. The standard IRS Plus deployment is configured to turn auditing on when an incident is first marked as Completed. It can be configured to start at any workflow stage, including at any custom workflow stages that may have been added.

1.3.5 API (APPLICATION PROGRAMMING INTERFACE)

IRS Plus includes an API for third party integration. The API is built on open standards used widely in the industry (SOAP Web Service). The API allows information to be pushed into IRS Plus from other systems.

1.3.5.1 CAD (C & C) INTEGRATION

The IRS Plus system is typically populated with data from a CAD system. This allows many of the questions to be pre-populated.

The system includes a standard SOAP-based API for CAD system integration to feed IRS Plus with incident data. Most current major CAD vendors have developed interfaces to IRS Plus using our API, we also have our own 'off-the-shelf' integrations for Remsdaq and Vision CAD Systems.

- Motorola Solutions Guardian Command (built in)
- SSS Public Safety (Motorola Solutions developed interface to Vision CAD)
- SysTel (SysTel developed interface)
- Intergraph (Intergraph developed interface)
- SEED (Seed developed interface).

If an FRS is not able to use one of these interfaces, an interface can be developed by the FRS, the CAD vendor or by Motorola Solutions. We are happy to discuss integration, and can quote for any integration work.

It is assumed that minimal configuration is required, such as configuring mappings between call sources or incident types. If more significant configuration or development is required, this may delay roll-out and require paid-for work at the standard rates.

1.3.5.2 CUSTOMISATION

The system is provided with the standard HO incident report form. Customers can add value to the IRS Plus incident data by capturing additional details on the incident report form. For example, this can be linked to specific campaigns or initiatives (e.g. Fire Safety) or to specific problems affecting your service (e.g. flooding).

The system can be tailored to capture virtually any additional details through customisation of the incident report form.

This is provided as an additional service, as described in the pricing schedule.

1.4 SYSTEM LOAD CAPACITY AND SCALABILITY

The system is scaled to provide access to a significant proportion of the Fire and Rescue Services, including all those currently using the HO's IRS system.

The expected system load is:

- Maximum of 400 users per FRS for IRS Plus form population (10,000 users total)
- Maximum of 10 HO users
- Maximum of 10 Motorola Solutions support users
- Maximum of 100 concurrent users.

If the number of customers exceed this, the system can be rapidly scaled to provide additional capacity.

2 IRS PLUS SERVICE SYSTEM DESIGN

IRS Plus is a SaaS / Cloud system hosted centrally on a proven platform and accessed by customers via the internet.

It is hosted on a Microsoft Azure platform and is accessed by customers across the internet.

Naturally the exact design of the system and the security measures are commercially sensitive information, and disclosure of this could affect the security of the system.

The application integration architecture is as follows:

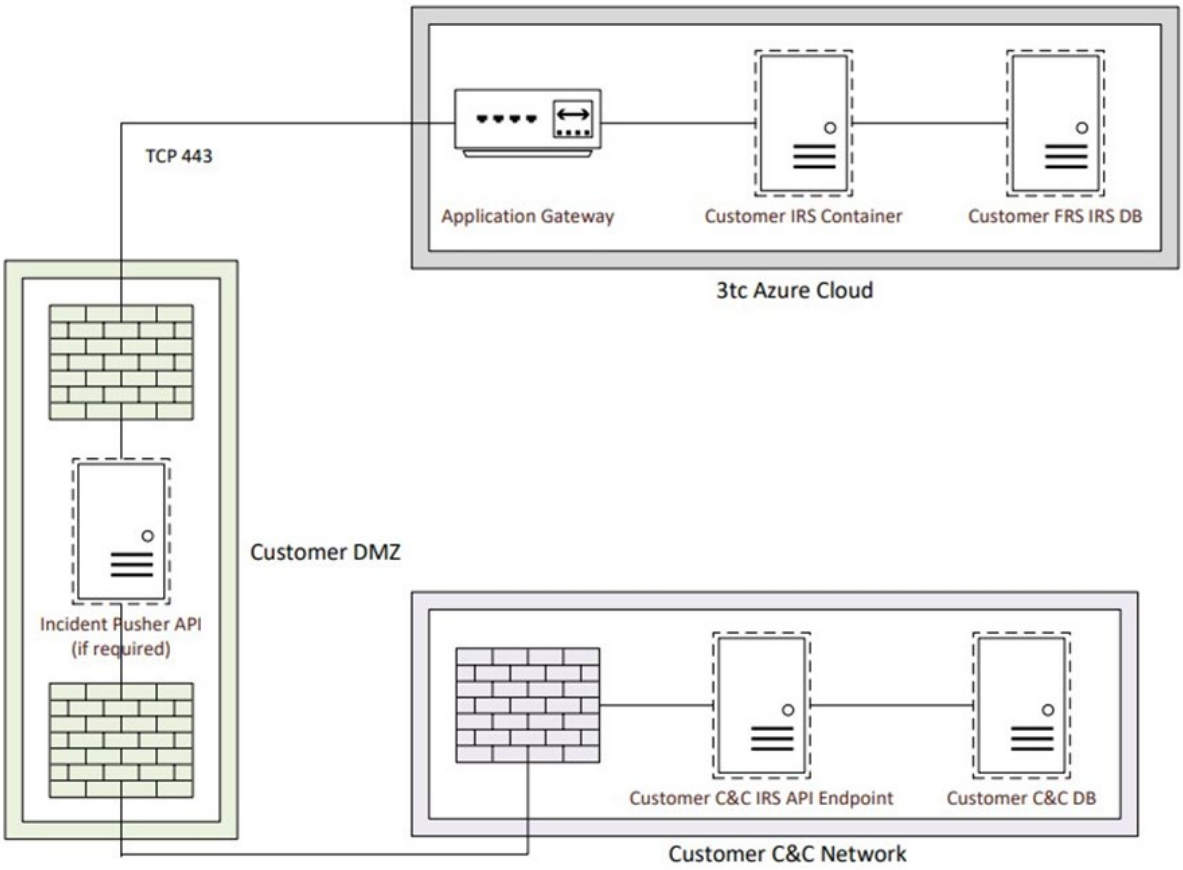


FIGURE 2 - INCIDENT TRANSMISSION WHEN CUSTOMER ENVIRONMENT CALLS FOR A PROXIED INTEGRATION VIA A DMZ

Incident Transmission when the customer environment allows HTTPS access to the C&C Network:

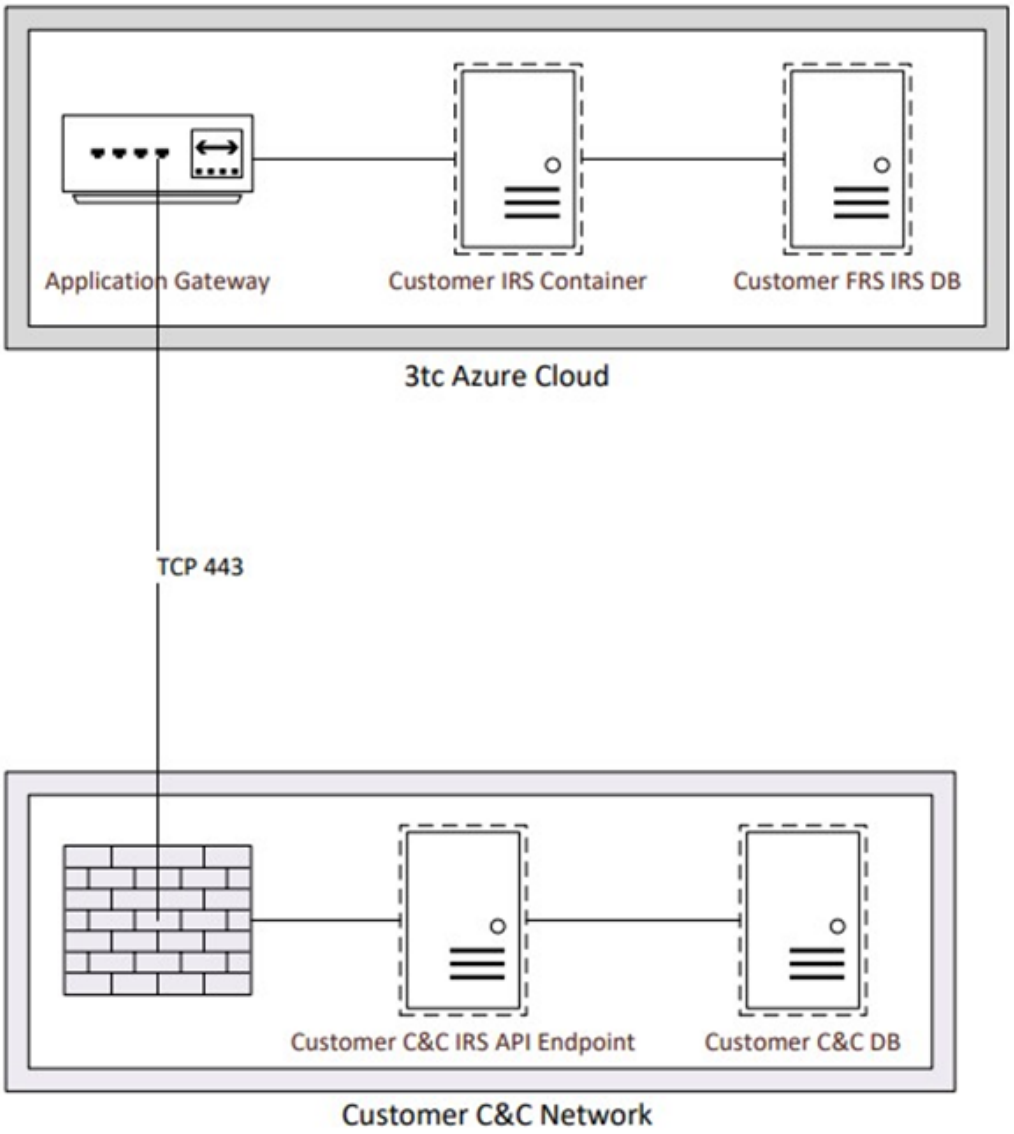


FIGURE 3 - INCIDENT TRANSMISSION WHEN THE CUSTOMER ENVIRONMENT ALLOWS HTTPS ACCESS TO THE C&C NETWORK

High Level Data Flow Overview from Incident creation within a C&C system, through the 3tc IRS application and finally into the Home Office IRS solution:

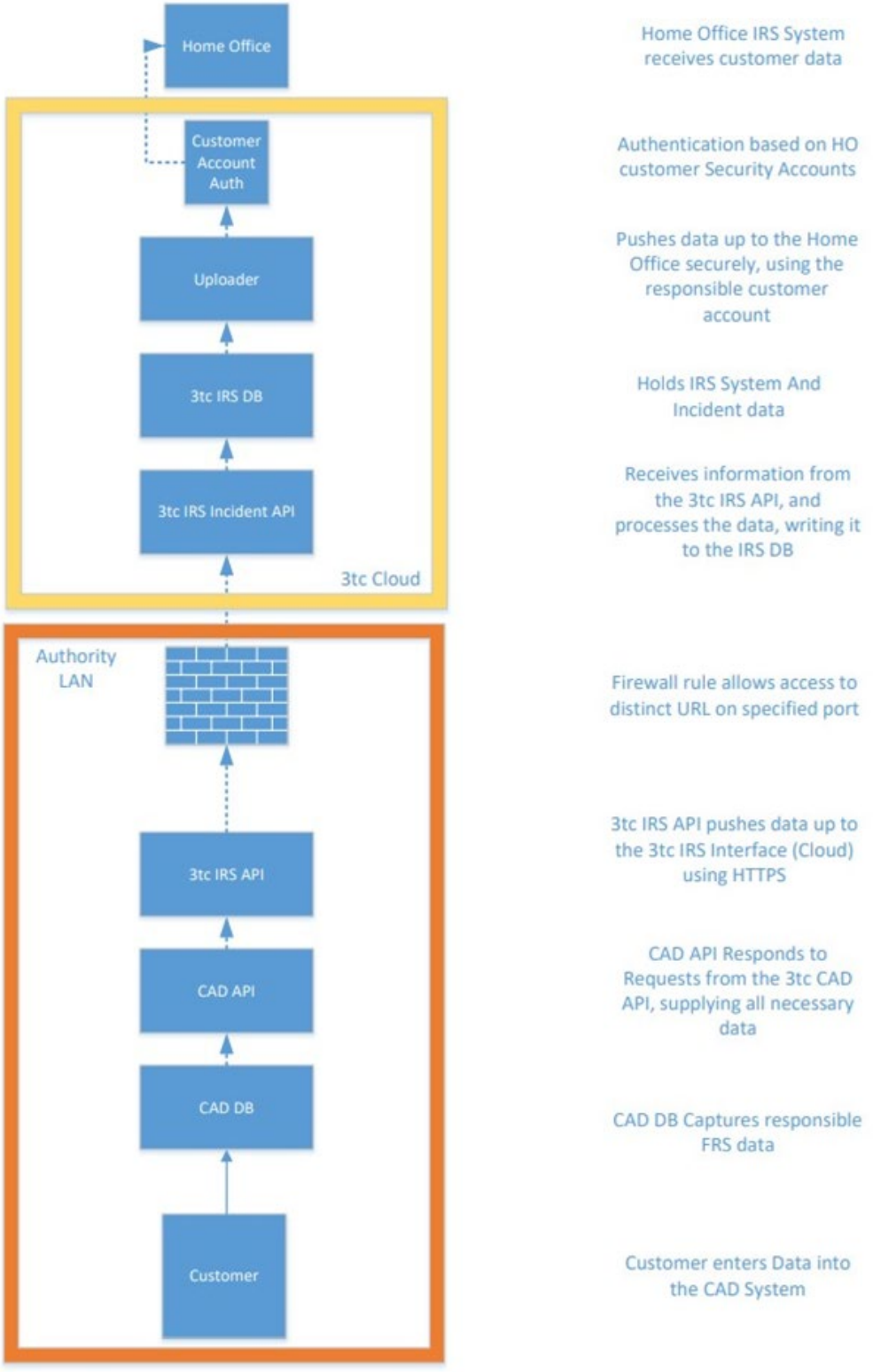


FIGURE 4 - HIGH LEVEL DATA FLOW OVERVIEW FROM INCIDENT CREATION WITHIN A C&C SYSTEM, THROUGH THE 3TC IRS APPLICATION AND FINALLY INTO THE HOME OFFICE IRS SOLUTION

2.1 FRS ACCESS / NETWORKING

The system uses a single top-level domain name (TLD). Each FRS accesses the system using a subdomain of this. For example, if the TLD is irsplus.org, a sub-domain for 'Anyshire FRS' may be anyshirefrs.irsplus.org.

The sub-domains are associated with the IP address of an IIS web server specific to each FRS via DNS.

2.2 SERVER ORGANISATION

2.2.1 APPLICATION SERVER

Each FRS system has up to two application servers. One for Live and one for Test (if applicable) This hosts the following components:

- Live/Test (if applicable) IRS Plus and Reports system (if applicable)
- HO Submission Service Interface (Live system only)
- Live/Test CAD API
- Live/Test (if applicable) IRS Plus Form Configuration Tool
- The server OS version used is the latest available from the hosting provider at the time of installation and is updated and maintained throughout the life of the service.

2.2.2 DATABASE SERVER

A single database server is used to host all of the databases required for all of the FRS systems. The database server is kept separate from the Web Server to provide additional security as such the data is not stored on an internet facing server. Additionally, the data can be backed up separately reducing backup and restore times.

The SQL Server version used is the latest available from the hosting provider at the time of installation.

2.3 CUSTOMER INSTALLED COMPONENTS

In order to use the system, customers may need to install some components on their system.

2.3.1 CAD INTERFACE

Customers using a Vision CAD System must install a CAD interface on their system. We will provide the installers for the application, and will provide consultation on the setup process. We can also perform the installation (charged at engineering day rate) however the customer will be responsible for providing an effective remote access method. The customer will be responsible for all networking adjustments to be undertaken outside of the 3tc Azure Network boundary.

Customers already using our 3tc CAD system will experience a fairly hands-off process outside of providing us with some data mapping details based on your data capture requirements and your bespoke custom data.

For 3rd party CAD providers outside of the ones mentioned above, we will expect said supplied to integrate to our standard IRS Interface API. During the early stages of your project, we will provide you and your CAD supplier with our API documentation for their development. Following the signing of NDAs between us and the relevant third parties.

2.3.2 WEB BROWSER

In order to access the system, customers must install a web browser compatible with IRS Plus (see Section 4.3 - Web Browser Compatibility). The installation and support of this is the responsibility of each customer.

2.4 SECURITY AND RESILIENCE

Security of the system is important as it contains potentially sensitive data. The system is secured as described below.

2.4.1 WEB TRAFFIC / DATA IN TRANSIT

All web traffic is secured by HTTPS – the system uses a wildcard SSL Certificate for the TLD. This includes client traffic and data sent to web services.

The SSL Certificate is provided and managed by a trusted certificate provider.

2.4.2 FIREWALL

The Azure hosting provides software firewall provision, which we configure to only allow the traffic required to access the IRS Plus system and the incoming and outgoing interfaces.

It is each customer's responsibility to configure their own firewalls and networks for access.

Access can be further locked down to allow access from the FRSs own IP addresses if required.

2.4.3 USER AUTHENTICATION

Users are authenticated using Forms authentication against credentials stored within the system. There are different credentials for the Live and Test environments. Passwords have to meet minimum complexity levels. User sessions automatically time out after a system-wide configurable time period.

We also offer SSO (Single-Sign On) integration to customers who using Azure Entra ID (previously Azure AD) endpoints that can be made available to our webservice. Our SSO integration provides full support for Microsoft MFA, allowing for easy on-boarding and end-user management. SSO integration replaces the above 'integrated' authentication method and instead uses your organisations own authentication server.

2.4.4 NETWORK / INTERNET SECURITY

The system undergoes annual penetration testing, which is performed against the server by a reputable third party. We resolve any issues that are identified that potentially allow sensitive data to be compromised.

The internal network on Amazon Web Services (AWS) is a private network, not accessible to the outside world other than via the defined entry points.

It is the customer's responsibility to ensure that the connections are secured at their end of the connection. For example, by ensuring browsers and operating systems are correctly patched and anti-virus and anti-malware software is used.

2.4.5 MONITORING

Access is monitored using the Microsoft Azure provided tools and infrastructure.

Additional monitoring and auditing is provided by the application layer logging infrastructure and event logs.

Where appropriate, automated notification of issues is provided to our support team to allow proactive resolution of security and resilience issues.

2.4.6 DATA SEGREGATION AND DATA ACCESS

All customer systems use a separate database and are therefore segregated from each other. Customers are not able to access each other's data via the web application.

Customers are not able to access the databases directly. All data access is via the supplied web applications.

Motorola Solutions is able to access all the FRSs' data for the purposes of delivering and supporting the system only. This is subject to Data Protection and Information Security policies covered under ISO 27001.

2.4.7 DATA STORAGE

2.4.7.1 DATA BACKUP, DISASTER RECOVERY AND RESILIENCE

Data is stored within the database server. No sensitive data is stored on the internet facing Web Server.

Data is backed up from the database server regularly using Azure automated backup systems. In between backups, transaction logs are recorded. This allows point in time recovery of the system and minimal data loss. Typically, Microsoft Azure 'point in time restores' provide restorations to within five minutes.

Data backups are only maintained for the purpose of recovery, and therefore only kept for a short retention period.

2.4.7.2 DATA EXTRACTION / REMOVAL

Should a customer decide to end their usage of the system, their data will be permanently removed from the system.

Their data is removed as follows:

- Data is removed by permanently erasing the databases from the system
- Backups of the databases are permanently erased (subject to the short retention period)
- Their Web Server virtual machine instance is shut down and erased
- Any user accounts or other access information used by the customer is removed.

Note: Once the retention period has passed, there will be no ability to restore the system.

Prior to the permanent removal of their system, the customer is given the opportunity to extract their data to enable them to migrate it to their own system. This will be subject to an administration charge at the prevailing contracted day rate. Note, for customers migrating to the self-hosted IRS Plus system, the migration will be included in the migration process and no separate administration charges will apply.

2.4.8 ASSET PROTECTION AND RESILIENCE

2.4.8.1 DATA CENTRE PROTECTION

Data centre protection is provided by Microsoft Azure as described in this Microsoft Learn Article:

https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure:

2.4.8.2 COMPLIANCE

“We design and manage the Azure infrastructure to meet a broad set of international and industry specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, and SOC 2. We also meet country-/region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Rigorous third-party audits, such as those done by the British Standards Institute, verify adherence to the strict security controls these standards mandate.

Secure data deletion is provided by Microsoft Azure as detailed in this Microsoft Learn Article: https://learn.microsoft.com/en-us/azure/security/fundamentals/protection-customer-data:

In particular:

”Data destruction: When customers delete data or leave Azure, Microsoft follows strict standards for deleting data, as well as the physical destruction of decommissioned hardware. Microsoft executes a complete deletion of data on customer request and on contract termination. For more information, see Data management at Microsoft.”

3 CUSTOMER SYSTEM ROLL-OUT (ON-BOARDING)

Two example options are provided below for the roll-out of systems to new customers.

- **Option 1 - Single customer roll-out at a time.** We roll-out one customer at a time, from end to end. This is designed for customers who sign up individually.
- **Option 2 - Multiple customer roll-out at a time**. We roll-out several customers simultaneously. This is designed for multiple customers signing up together as part of a region or other consortium.

The options below are indicative only, and the roll-out process can be tailored for individual customers to meet their requirements.

3.1 COMMON ELEMENTS

The following elements are common to all roll-out options.

3.1.1 TRAINING COURSES

The following courses are provided:

- IRS Plus Forms Completion, Validation, Checking, Submission (approx. 4-6 hours)
- IRS Plus Reports (approx. 3-5 hours)
- IRS Plus Administration (approx. 1-2 hours).

These are typically provided over a two-day session, with the courses running on concurrent days.

3.1.2 DOCUMENTATION PROVIDED

We supply the following documentation:

- IRS Plus User Guide
- IRS Plus Reports User Guide
- API Technical Documentation
- SSO, Azure AD (Entra ID) Integration Guide (If Required).

3.1.3 USER AND ACCESS CONFIGURATION

We provide an admin login for each FRS to allow them to manage users and security.

In order to set the users up, we allow the following options, which should meet all FRSs needs.

We can also provide SSO integration to customers who using Azure Entra ID (previously Azure AD) endpoints that can be made available to our webservice. Our SSO integration provides full support for Microsoft MFA, allowing for easy on-boarding and end-user management.

3.1.3.1 MANUAL CONFIGURATION

The FRS configures their own users manually, using the web interface built into the system. The FRS will need to configure each user and their access level.

3.1.3.2 IMPORT USERS

Motorola Solutions imports users into the system based on a list provided by the FRS. For each level of user (level 1 to 3), the FRS will provide a list of usernames and passwords.

Note that the FRS can still manually configure the users after this point.

3.2 ROLL-OUT PROCESS – OPTION 1: SINGLE CUSTOMER AT A TIME

Option one is based on our traditional single-site roll-out process. This process is designed where single customers sign up to the IRS Plus service.

STAGE 1 PRE-SET UP (TIMESCALES 2-3 WEEKS)

During this phase we pre-set up all of the core components:

- Web Application Virtual Server base image
- SQL Server and all databases
- Creation of any necessary configuration scripts
- Creation of data migration scripts (costed option).

STAGE 2 CONFIGURATION OF LIVE AND TEST SYSTEMS (TIMESCALES 3-5 DAYS)

- Scripted configuration of FRS system
- Initial data load using Home Office IRS API – 3tc download your incident data from the Home Office servers so it's visible and editable in 3tc cloud IRS
- Set up users – create from Pro-forma from FRS (see below)
- Configure CAD interface to support any translations required
- Test CAD integration, and perform application UAT.

STAGE 3 END USER TRAINING (TIMESCALES 2-3 WEEKS)

- Train the trainer courses delivered
- FRS rolls out training internally, see below.

STAGE 4 GO LIVE (TIMESCALES 1-3 DAYS)

- 3tc wipe all incident data from your 3tc Cloud IRS system
- FRS stops using non-3tc BI system
- 3tc perform a final download of your data from the Home Office IRS API (or a fresh reimport of 3rd party system data)
- Enable CAD interface
- Go Live.

3.2.1 TRAINING FOR ROLL-OUT OPTION 1

We have assumed that training will be performed for individual FRSs as part of the roll-out process. Motorola Solutions train the FRSs' training staff, who cascade the training.

The courses are delivered at FRS premises, by our trainer. The training is performed using the FRS's own system (the hosted test system).

For each course we train a maximum of six people. The courses are held over two consecutive days. Additional courses can be run for more people, and these can be quoted separately.

3.2.2 OPTION 1 ROLL-OUT CAPACITY

With the plan defined above, it is possible to roll-out individual customers over a ten working day period (two weeks). Typically, we expect that we can roll-out up to three customers per month.

This does not include time for FRSs to internally roll-out training. Based on our experience it takes an FRS two to three weeks to roll-out training internally, due to shift patterns.

The plan below shows what a roll-out plan might look like. This is best case and assumes that FRSs are ready with training and with configuration data, and that there are no slippages. It also does not take into account bank holidays or other possible interruptions.

Activity	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23
Stage 1 Initial Set Up																							
Stage 2 Set Up system																							
Stage 3 Customer Training Roll Out																							
Stage 4 Go Live																							

FIGURE 5 - EXAMPLE ROLL-OUT PLAN

3.3 ROLL-OUT PROCESS – OPTION 2: MULTIPLE CUSTOMERS AT A TIME

Option 2 is designed to maximise the roll-out capacity to customers in order to shorten the time taken to roll-out to customers as quickly as possible. This roll-out process is designed where multiple customers sign up to the IRS Plus service together, such as part of a regional group or other consortium.

STAGE 1 PRE-SET UP (ONE TIME, TIMESCALES 2-3 WEEKS)

During this phase we pre-set up all of the core components and all of the customer systems:

- Web Application Virtual Server base image
- SQL Server and all databases
- Produce the scripts to configure all the customer systems
- Roll-out and configure customer systems
- Creation of data migration scripts (costed option).

STAGE 2 BULK FRS TRAINING (ONE TIME, TIMESCALES 2 WEEKS)

We run a bulk training course to train as many people as possible in the shortest period of time. This will be in the format of train-the-trainer. We hold four courses of up to 6 people (such as one person per customer), in a classroom scenario with two of our trainers. This is over two days and will cover all of the courses.

The customers then roll-out internally to their staff. Customers can do this in parallel with each other.

STAGE 3 FRS CAD INTERFACE AND USER CONFIGURATION (PER CUSTOMER, TIMESCALES 5+ DAYS)

The speed at which this can be done will depend on how prepared the customers are with the information required. If the customers are able to provide the necessary configuration information and arrange for testing of the CAD interface, we can configure a system in five working days.

We would intend to have slots available that customers can book to allow them to plan for the go live. Slots would be available on a first-come-first-served basis.

STAGE 4 FRS GO LIVE (PER FRS, TIMESCALES 1-3 DAYS)

This phase can be overlapped with the configuration phase. Once the FRS has completed configuration and training, the system can go live.

We would intend to have slots available that customers can book to allow them to plan for the go live. Slots would be available on a first-come-first-served basis.

Activities:

- 3tc wipe all incident data from your 3tc Cloud IRS system
- FRS stops using non-3tc BI system
- 3tc perform a final download of your data from the Home Office IRS API (Or fresh re-import of 3rd party system data)
- Enable CAD interface
- Go Live.

3.3.1 OPTION 2 ROLL-OUT CAPACITY

With the plan defined above, there is a longer initial deployment time, due to the up-front configuration and training.

The training and configuration phases are then performed in parallel, potentially significantly reducing time. All that remains then is the go-live phase, which can be rolled out within two working days per customer.

The following plan is an example roll-out plan. This is best case and assumes that customers are ready with training and with configuration data, all customers are available to do installations within a timely manner and time slots were booked with no gaps and that there are no slippages. It also does not take into account bank holidays or other possible interruptions.

Activity	W 1	W 2	W 3	W 4	W 5	W 6	W 7	W 8	W 9	W 10	W 11	W 12	W 13	W 14	W 15	W 16	W 17	W 18	W 19	W 20	W 21	W 22	W 23
Stage 1 Initial Set Up																							
Stage 2 Bulk Training																							
FRS Training Roll-out																							
Stage 3																							
Configure System																							
Stage 4 Go Live																							

FIGURE 6 - EXAMPLE ROLL-OUT PLAN

3.4 ROLL-OUT ASSUMPTIONS

In order to make the provisioning and transitioning as rapid as possible for new customers, Motorola Solutions has made various assumptions:

- There is no requirement-based acceptance testing for individual customers, any quality acceptance testing is done by the FRS on their own timelines. The system is provided as-is, and therefore we will only accept any issues raised that pertain to faults in the system or relating to any faulty configuration customisations for a particular customer.
- No incidents are imported from existing systems, including the current HO system (available as a service)
- The CAD interface is standard and does not require any development or significant modifications
- The customer / CAD vendor is able to provide all the information at the start of the process (e.g. user lists, interface configuration information)
- Each customer system is configured identically in terms of question configuration, validation rules and so forth
- Each customer may require their CAD vendor to do some installation or configuration. This is the responsibility (in terms of cost and effort) of each customer.
- Each customer may require configuration of their internal systems (such as networking, firewalls, CAD systems). This is the responsibility (in terms of cost and effort) of each customer.

If customers have a more relaxed timescale, then we can include extra services such as customisations and data transfer in the migration process.

4 SUPPORT

We provide technical support between the hours of 0900 and 1700 Monday to Friday. This excludes bank holidays and the days between Christmas and New Year.

Support is provided via a support telephone number, automated ticketing system and self-service portal. Urgent issues should be raised by telephone. Issues raised by email or by the portal generate an auto-response email, acknowledging that the issue has been raised and issuing a unique incident number. The incident is then managed by the support team in-line with your contractually defined SLA's.

Support is primarily provided from our company premises in Desford, Leicestershire.

All support is remote, as there is no facility to physically attend the Azure hosting environment. Support provided to FRSs is also remote.

Our helpdesk / support service accepts reports of:

- System non-availability
- Verified software faults
- Reporting of issues that are reasonably thought to be software faults.

All questions regarding the HO specific elements, such as how to answer HO's questions or clarification around the HO process should continue to be directed to the HO's helpdesk as normal.

4.1 QUESTION AND VALIDATION RULES CHANGES

We support adding and changing of questions and validation, including adding additional sections to the IRS Plus Form to collect data outside of the HO required questions.

Note that the questions and validation configuration must support the submission of valid information to the HO.

4.1.1 HOME OFFICE CHANGES

We configure reasonable changes to the standard HO questions and validation rules as part of annual support. We have an annual nominal budget for these changes, after which, changes are chargeable at our standard day rate (or quoted for larger scale changes). Turn-around time for configuration changes is typically four to eight weeks from agreement of scope. Timescales may be longer for larger scale or more complex changes.

Changes are configured by Motorola Solutions on behalf of our customers. We assume that changes required by the HO are applied to all customer systems (Live and Test).

It is worth noting that if the HO drastically change their solution and we are required to re-design our integration; these timelines may well extend. Our annual change scope is limited to configuration, not development.

4.1.2 FRS CHANGES

Minor changes to question configuration and validation specific to individual customers are carried out as part of annual support. This is limited to two days of engineering time per customer, after which changes are chargeable at our standard day rate (or quoted for larger scale changes).

This does not include the creation of lookup tables within the IRS database. As the customer will not have “write” access to the database, when a custom question in the Incident Form requires a new lookup table in the database, the customer will need to raise a request to our support team, using the same methods as if you were to report an incident. Please note, that these changes need to be planned in and may also be subject to our internal CCB (Change Control Board) for planning.

Turn-around time for configuration changes is typically two to four weeks from agreement of scope. Timescales may be longer for larger scale or more complex changes.

Changes are configured by Motorola Solutions on behalf of the FRSs.

4.2 SOFTWARE RELEASES

Motorola Solutions typically releases updated versions of the software on a six-monthly basis. The software updates include a roll-up of any new features and bug fixes made during the preceding period.

It may be necessary to release software more frequently than the six-monthly schedule. For example should the need arise to address a serious issue, a patch release may be released quickly and directly to the live systems of affected customers.

4.2.1 SOFTWARE TESTING

Software is tested internally prior to release by our internal test resource. This includes a mixture of automated low-level testing (unit testing) and manual user testing against defined test scripts. The test scripts are designed to test the software to prove functionality and to test issues that have been resolved.

Once the release is signed off internally, it is deployed to the customers’ Test systems (if purchased). If you do not purchase a test system, you will receive release notes at the same time customers with a test system do, in order to give you early sight of the upgrade. It is then available for a period of one month for familiarisation and testing, again for customers with a test system. After this preview period it is installed on the live system. We resolve any serious issues reported during the preview period prior to release, which may cause a delay of the release to the live system should further testing or development be required.

4.3 WEB BROWSER COMPATIBILITY

IRS Plus is currently compatible with the following browsers:

- Microsoft Edge
- Chrome 43
- Specifying support for Edge and Chrome (Chromium Based Browser) versions is more difficult because of the frequent and transparent upgrades. Our aim is to provide ongoing support for Edge and Chrome, but we are unable to guarantee this.

Whichever browser is used, HTTPS, JavaScript and download functionality must be enabled.

4.4 SUPPORT SLAS

The period during which the Contractor provides System support shall be office hours only from 0900 to 1700 hours from Monday to Friday excluding Public Holidays and weekdays between Christmas and New Year.

4.4.1 TARGET RESPONSES

These are our target responses (office hours only):

PRIORITY CATEGORY	PRIMARY RESPONSE	RESTORATION OF SERVICE
1	15 minutes	8 hours
2	1 hour	4 business days
3	1 business day	Next release

4.4.2 PRIORITY CATEGORIES

REPORT CATEGORY	DESCRIPTION
1	A single fault preventing the use of core features for all users, or which causes substantial downtime of the system or severe performance degradation
2	A single fault preventing the use of core features for multiple users (over 50% of all users)
3	A single fault preventing the use of core features for one user; or A single fault preventing the use of secondary features for multiple users; or A single fault preventing the use of secondary features for one user; or A single fault of cosmetic of minor nature affecting any number of users; or A documentation or non-functional error that does not impact upon the operation of the software.

4.4.3 DEFINITIONS

TERM	DEFINITION
PRIMARY RESPONSE	Contact from the Contractor's Support Division to clarify the problem and discuss potential actions that can be taken immediately
RESTORATION OF SERVICE	An acceptable temporary work around into the problem that allows the users to operate the system without substantial degradation in performance. A temporary fix will only be applied where suitable. In some instances a temporary fix may not be available.

4.4.4 SCHEDULED MAINTENANCE

We perform scheduled maintenance on the system from time to time in order to optimise performance, resolve issues, update data sets (such as gazetteers) and update system components.

We plan these events on a quarterly basis, and FRSs are notified in advance of the date and estimated duration of the downtime.

4.4.5 UNSCHEDULED MAINTENANCE

The system is robust and stable, having been in service for many years in live environments. However, we do anticipate that there may be instances where there are unplanned events where the system is unavailable for extended periods of time.

In such events we will work to resolve the system issue as quickly as possible. If the downtime looks like it may be protracted, Motorola Solutions will notify the FRSs' primary contact and advise them of the status of the ongoing incident.

4.4.6 SERVICE AVAILABILITY

The system availability we aim for is 99.9%. This allows for average unplanned down-time as follows:

8.76 hours per year	43.8 minutes per month	10.1 minutes per week	1.44 minutes per day

Availability is measured per end-user FRS, not across the entire system and does not cover planned down-time for maintenance as defined in 4.4.4 Scheduled Maintenance.

4.5 RESILIENCE

The Microsoft Azure hosting provides backups of SQL Server as follows:

- Daily instance backups
- Five minute transaction logs.

This allows point in time recovery in the event of a database server loss. The loss of a server is anticipated to be extremely low.

4.6 EXCLUSIONS

We do not answer any questions on the HO-defined questions, how to answer them or general questions about how to answer questions in the form.

We are not able to support issues with the individual customers' environment or infrastructure.

5 PRICING

All costs are exclusive of VAT.

The costs provided have assumed a minimum contract length of three years. Extensions are available.

In order to have efficient and predictable costs, the AWS hosting must be paid for in advance. In order to allow for initial configuration and deployment of the system, the hosting would need to start from the configuration phase of the contract. Therefore, the three-year duration would start from the point in time where the contracts are signed off and the hosting provisioning begins. Therefore FRSs which come on board after the initial provisioning may not get a full three years' service.

For the purposes of costs, we have assumed the AWS hosting will be in the Europe (Ireland) region.

5.1 IRS PLUS ANNUAL PRICES

Please refer to separate price list.

5.2 MICROSOFT LICENSING

AWS licensing for MS SQL Server and MS Windows is included in the hosting costs.

5.3 OS ON-DEMAND AND OS ADDRESSBASE PREMIUM

It is assumed that end-user organisations are FRSs covered by an OS Public Sector Mapping Agreement (PSMA) allowing free access to OS On-Demand. This is subject to Ordnance Survey's Fair Usage Policy. The system will be configured with your unique API key (available from OS), which will allow provide access to the mapping service under your existing PSMA. Note that any usage outside of the Fair Usage policy or exceeding the free entitlement, or outside the PSMA (and any resulting charges from OS), will be the responsibility of each customer.

5.4 GENERAL CAVEATS

All IPR for the software designed and developed by Motorola Solutions will remain with Motorola Solutions. This includes the application software, database design, overall solution design and any other IP pertinent to this solution.

Each Fire and Rescue Service will require a licence which will cover them for their current geographical area of operation and they will be required to sign an end user licence agreement as detailed in the contract document.