
SFM Research Handbook

Sep 08, 2023

1	Research Handbook for Security Force Monitor	1
2	Research methodology	3
3	Tutorials	7
4	Countries	9
5	What data does the Monitor collect?	19
6	Data integrity measures	21
7	Units	25
8	Persons	47
9	Persons Extra	61
10	Incidents	69
11	Locations	85
12	Sources	105
13	Frequently Asked Questions about WhoWasInCommand	119
14	Unit Records on WhoWasInCommand	125
15	Person records on WhoWasInCommand	133
16	Incident Records on WhoWasInCommand	139
17	What data can I download from WhoWasInCommand?	143

Research Handbook for Security Force Monitor

1.1 About Security Force Monitor

The Security Force Monitor works to make police, military and other security forces around the world more transparent and accountable.

Human rights researchers, journalists, advocates, litigators and others engaged in making security forces accountable face a common problem – a lack of clear, detailed information on those forces. Often, answering even simple questions can be difficult:

- Who is in charge of the specialized anti-riot police unit?
- What army unit has jurisdiction over what areas?
- Where did this commander previously serve?
- When was a particular police unit based in a specific city?

There is a vast amount of public information on security forces around the world, but it is unstructured and scattered among a wide variety of sources, making it prohibitively costly for those engaged in public interest work to understand the security forces of a particular country.

The Security Force Monitor aims to solve this problem and aid those working to make police, military and other security forces accountable. The Monitor analyzes and compiles public information to provide data on: the command hierarchy, location, areas of operation, commanders and the other linkages between units – all tracked through time. The Monitor's mission and technical offerings have been developed to serve, and in consultation with, a wide range of civil society efforts.

The Security Force Monitor is a project of the [Columbia Law School Human Rights Institute](#).

[More information about Security Force Monitor](#) can be found on our website.

1.2 About this Research Handbook

This Research Handbook is a guide to investigating the structure, personnel, infrastructure, operations and connections to human rights abuses of security forces around the world. It provides detailed information about the methods, data and tools used by Security Force Monitor to do this.

The Research Handbook has three sections:

- **WhoWasInCommand.com User Guide:** The data created by Security Force Monitor is published online at <https://WhoWasInCommand.com>, a purpose-built platform with powerful search functions, clean and interactive views of the organizational structure, command of personnel and chains of command, and the geographical footprint of security forces in many countries.
- **Methodology:** Security Force Monitor has a four phase approach to researching a country's security forces. This section outlines our process.
- **Data Model:** this section describes the way that Security Force Monitor structures the data it collects and the steps taken to ensure data integrity. In this section, we also provide detailed documentation about the standard data collection formats and fields that we use to organize our research and store data:
- the *Persons* and *Persons Extra* formats are used to capture data about persons, their ranks and roles within security forces, information about their online presence and how they look and sound.
- the *Units* format is used to stored data about the organizational structure of a security force, its physical infrastructure and its areas areas of operation.
- the *Incidents* format is used to store data about human rights abuses specific units or persons from security forces are alleged to have committed.

This Research Handbook is a work-in-progress and is regularly updated during the course of the work of Security Force Monitor.

1.3 Contributors

Tony Wilson, Tom Longley and Michel Manzur from [Security Force Monitor](#) are the authors of this Research Handbook.

Security Force Monitor has partnered with [DataMade](#) to create WhoWasInCommand.com. DataMade has operationalized and refined Security Force Monitor's data structure, worked with us to create a powerful open source platform to put the data online, and made a significant contribution to the concept and design of WhoWasInCommand.com.

[James McKinney](#) - at the time with [OpenNorth](#) - was a major contributor to the development of Monitor's data model, adapting Popolo (an international open government data standard) and developing the specifications for the Monitor's research tool.

1.4 Copyright and license

The Security Force Monitor Research Handbook is licensed under a [Creative Commons Attribution 4.0 International License](#). You are free to copy, share and adapt all or any part of this handbook, but you must give appropriate credit to Security Force Monitor.

Fig. 1: License: CC BY 4.0

Research methodology

Security Force Monitor follows a four phase process when researching the security forces of a country.

2.1 Phase 1: Scope out sources

General sources

Security Force Monitor collects data about the *Persons* and *Units* that comprise security forces, along with allegations of human rights abuses made against security forces. This data is carefully collected from a variety of sources, generally online. These include:

- Laws of the country;
- Official government media;
- Press releases from the relevant ministries of the country (Information, Defense, Interior, and others);
- Security force newsletters;
- Social media pages for security services or government agencies;
- Statistics and data agencies;
- Local government websites;
- Human rights commissions;
- Third country government publications and other documents;
- United Nations publications and other documents;
- Local news reportage;
- Civil society and human rights reporting;
- Academic research; and,
- Other country specific sources.

The Monitor also identifies non-digital resources such as monographs, scholarly literature, biographies and other materials about security services. The existence and availability of these type of sources vary widely from country to country.

State administrative structures and geography

Security Force Monitor researchers familiarize themselves with the country's governance and administrative structures, gaining understanding about the levels of government (for example: local, regional, state, national) and their connection to different security forces. In examining this we also flag where there might be major changes in the structure of government, such as those that may accompany a constitutional referendum or a peace process. These affect how the Monitor will represent data on security forces over time.

Examining the administrative geography of a country provides important context for the structure and operations of the security forces. This part of the scoping process also gives us insight into how much of a country's administrative geography is represented in online gazetteers (like [OpenStreetMap](#) or [GeoNames](#)) that the Monitor uses in its analysis.

Potential high value datasets

During this first phase, researchers also identify sources that could be turned into large, high value datasets for the Monitor. These are sources that contain a sufficiently large amount or complex type of data that technical help is necessary to extract it in a timely way; doing the work "by hand" is possible, but would be slow and error prone. These high value data extraction tasks use techniques such as web-scraping, scripted parsing and geospatial analysis. An example of these types of sources are the [Internet Archive snapshots the official webpage of the Mexican Army and Air Force](#) (and child pages) going back more than a decade which outline the top level structures of the Mexican army and its commanding officers.

2.2 Phase 2: Write a Country Guide

The sources gathered during our scoping phase are used to write a Country Guide to assist with further research.

The Guide begins as a general overview of the structures of security services of a country. It gives researchers a general framework to help organize and prioritize research, by giving an estimate of the scale of the work: number of installations, units, persons that need to be researched in detail.

For example, the Monitor's scoping research on Nigeria revealed that by law every state and the federal territory has a Police Command. By extension this means since 1996 (when the last states of Nigeria were created) there have been 37 Police Commands. Statistics from the Nigeria Police Force show that between 2007 and 2012 most Police Commands were in charge of 2 to 3 Police Area Commands (though some heavily populated states have more, with Lagos having the most at 8). These statistics also show that on average each state and the federal capital territory had 30 Police Divisions, which by law are generally under the command of a Police Area Command. Thus, from a few initial sources a Monitor researcher can have a general sense of the structure of the police and a useful metric to compare the Monitor's dataset against.

Further, a list of keywords and sources is created for researchers as well - these serve as leads for researchers to follow.

This Country Guide is updated as new details on the security forces are discovered through the course of the Monitor's work.

2.3 Phase 3: Conduct detailed research

Researchers use the initial keywords and sources to begin a "deep dive" into the security forces.

Anything relating to the types of information the Monitor collects is entered into the Monitor's database. The Data Model section of this Research Handbook gives detailed guidance to Monitor researchers about the types of data to take from sources and how it should be entered.

Additionally, data from this research is used to update the Country Guide to provide greater granular detail on the security forces of a country or to update sections as needed. New sources and keywords discovered during research are added to the existing guide as well.

As the Monitor builds its database on the security forces of a country, new information is cross-referenced to further evidence data, discover gaps, or identify mistakes. There are three key questions Monitor researchers ask themselves whenever they review information in a source:

- “Does this make sense given what is detailed about the security forces from other sources?”
- “Is it possible this source is correct and our other sources are incorrect?”
- “Do I have enough information to accept or reject what this source says?”

The Country Guide acts as a framework for researchers to understand the security forces and to help a researcher answer these questions. Data entered into the Monitor’s databases are progressively updated as new information is found. Throughout, researchers take a number of quality assurance steps to validate the data against the standards set out in the Data Model section

2.4 Phase 4: Publish data

Researchers will publish data online when confident that the main branches and overall structure of a country’s security forces are adequately covered. Data is published online on the Monitor’s platform: WhoWasInCommand.com.

3.1 Recording geographical information

Guidance on how to analyse, extract and record geographical information from sources used to create our data.

3.2 Dates and time periods in Security Force Monitor

Guidance on how Security Force Monitor deals with time in the datasets

3.3 Archiving and retrieving sources from the Internet Archive

Guidance on how to create an archive snapshot of a source using the Internet Archive, and how to retrieve that information.

WhoWasInCommand.com currently hosts data on the below countries.

4.1 Bangladesh

4.1.1 Bangladesh: Overview of Coverage

The Security Force Monitor's current dataset is focused on the structure of police in Bangladesh. Additional research (detailed below) will focus on other elements of the security forces of Bangladesh.

4.1.2 Bangladesh: Administrative Division

Bangladesh is divided into 8 Divisions which are further divided into 64 Districts and then 491 Upazilas.

4.1.3 Bangladesh: Police

The Bangladesh Police is the national police force of Bangladesh, overseeing all branches of the police. The Bangladesh is divided into the Special Branch, Criminal Investigation Department, Rapid Action Battalions, and Ranges (which oversee police forces across large geographic areas and are further divided into District Police, Circles and Police Stations) and an Armed Police Battalion. Specialized branches of the Bangladesh Police include the Highway Police, Industrial Police and Railway Police. Additionally, the Bangladesh Police has several Metropolitan Police forces for the major cities of Barisal, Chittagong, Dhaka (the capital), Khulna, Rajshahi, and Sylhet. Each Metropolitan Police is further divided into Divisions, Zones and Police Stations.

4.1.4 Bangladesh: Outstanding Areas for Further Research

- Detailing commanders of Bangladesh Police across various units and branches.
- Identifying locations and areas of operations through time of Bangladesh Police units.

- Building command hierarchy of the armed forces of Bangladesh and identifying location and area of operations of various units.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Bangladesh.

4.2 Egypt

4.2.1 Egypt: Overview of Coverage

The Security Force Monitor's current dataset is a "snapshot" of the structure of the police in Egypt as of September 2016 and military forces in 2011. Additional research on Egypt is dependent on funding and priorities of partners concerned about the human rights practices of the security forces of Egypt.

4.2.2 Egypt: General Background on Security Forces

Egypt has security forces with different responsibilities for internal security. Crime fighting is the prime responsibility of the General Investigations Police. The Central Security Forces (CSF) are tasked with policing public events and demonstrations, but may also be used in other internal security operations.

4.2.3 Egypt: Administrative Division

Administratively, Egypt is broken up into 27 governorates each of which is headed by a governor who is appointed by the president. The number of governorates has varied over time, with several governorates being created and then disbanded in recent years.

4.2.4 Egypt: Security Forces

Police (General Investigations Police)

The General Investigations Police is the national police force of Egypt. The President of Egypt is the supreme commander of the police, which are housed inside of the Ministry of Interior. Police in each governorate are under the command of the Security Directorate of that governorate (headed by a Security Director) who in turn reports to the Governor. Organizationally, most police operate from one of the approximately 1700 Police Stations. Central Security Forces

The Central Security Forces (CSF) is a specialized force focused on "anti-riot" activities, meaning they are generally deployed to police protests or other public gatherings. The CSF sits inside of the Ministry of Interior.

Egyptian Armed Forces

The Egyptian military, particularly the army, plays a key role in politics and general security affairs. There are four major branches of the military, the Army, the Air Force, Air Defense Force and the Navy, all of which fall under the Ministry of Defense. Operationally, the main formations of the army are the Field Armies and Military Zones. Smaller units that report up to the relevant Field Armies or Military Zones are Divisions, Brigades and Battalions.

4.2.5 Egypt: Outstanding Areas for Further Research

- Expanding the command structure of the General Investigations Police, Central Security Forces and Egyptian military through time.

- Detailing commanders of the General Investigations Police, Central Security Forces and Egyptian military across various units through time.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Egypt.

4.3 Mexico

4.3.1 Mexico: Overview of Coverage

The Security Force Monitor's current dataset comprehensively covers the command structure, locations and areas of operation of the Mexican armed forces from roughly 2006 to 2018. The Monitor has extensive data on commanders, though some smaller units have gaps. Finally our data includes a "snapshot" of the command structure and locations of Policía Federal units as of June 2016. Additional research (detailed below) will focus on other elements of the security forces of Mexico.

4.3.2 Mexico: General Background on Security Forces

Mexico has several layers of security forces. Crime fighting generally falls to local, state and federal police forces, each with their own chain of command. Specialized agencies within or independent to these police forces are also involved in crime fighting. Additionally, the armed forces of Mexico have been increasingly involved in internal security operations.

4.3.3 Mexico: Administrative Division

Mexico has a federal structure. There are 31 states as well as a federal entity of Mexico City. Each state is subdivided into municipios of which there are 2,456. Mexico: Security Forces

Police

Mexico has federal, state and municipio (municipal) police forces as well as a separate police for the federal capital. At the federal and state level police forces are generally divided by role and command structure into policía preventiva (preventive police) in charge of maintaining order and usually under the command of the Secretaría de Seguridad Pública (Ministry of Public Security) and policía judicial (judicial police) usually under the command of the state Procuraduría General de Justicia (Attorney General).

The size and structure of Policías Municipales (municipal police) can vary widely. Generally, they are under the command of the Presidente Municipal (municipal president, also informally referred to as the Alcalde or mayor) of the municipio which they operate. Not every municipio has a police force, however. Some states in Mexico are dissolving their municipal police forces in favor of newly created state-level forces while other states are establishing new state-level forces which control existing municipal police forces.

Mexican Armed Forces/Military

The President of Mexico is the Commander-in-Chief of the Mexican Armed Forces, which are divided into the Army and Air Force under the command of the Secretaría de la Defensa Nacional (SEDENA) and the Navy and Marines under the command of the Secretaría de Marina (SEMAR). SEDENA also includes the Special Forces, and Military Police. SEMAR contains its own infantry and air forces as well. Both SEDENA and SEMAR include an Estado Mayor (General Staff) that play an active role in the chain of command between the secretary and operational units. Army

The Mexican Army is broken up into several Regiones Militares (Military Regions) which usually cover several states and oversee Zonas Militares (Military Zones) which usually operate within one state or in portions of two or more states. Below the Zonas Militares are smaller units: Batallones de Infantería (Infantry Battalions), Regimientos de

Caballería Motorizado (Motorized Cavalry Regiments), Regimientos de Artillería (Artillery Regiments), Guarniciones Militares (Military Garrisons), and several other groupings, all of which are generally under the command of a Zona Militar.

Air Force

The Mexican Air Force is also divided into geographic Regiones Aéreas which command Bases Aéreas. Bases Aéreas in turn command Escuadrones Aéreos.

Navy/Marines

Similar to the Army, the SEMAR is broken into several Regiones Navales (Naval Regions) which command Zonas Navales (Naval Zones). SEMAR also includes two Fuerzas Navales (Naval Forces). The Navy has been very active in internal security operations, mainly through the deployment of the marines, which are generally grouped into Brigadas de Infanteria de Marina (Marine Brigades) and smaller Batallones de Infantería de Marina (Marine Battalions). Since 2007 the command structure of the marines has been restructured several, but currently marine units are generally under the command of a Zona Naval or Región Naval.

4.3.4 Mexico: Outstanding Areas for Further Research

- Expanding the command structure of the Policía Federal through time.
- Detailing command structures, locations and areas of operations for state and municipal police forces in various states of Mexico through time.
- Identifying additional details on individual units and personnel as needed to fill any gaps in the records of units and commanders of the armed forces of Mexico during the timeframe of 2006 to 2018.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Mexico.

4.4 Myanmar

4.4.1 Myanmar: Overview of Coverage

The Security Force Monitor's current dataset is focused on the army structure, location and area of operations from 2000 to 2018. Additional research (detailed below) will focus on additional elements of the security forces of Myanmar. **General Background on Security Forces**

The Tatmadaw, or armed forces of Myanmar, play a central role in internal security and politics. The military has directly ruled Myanmar and remains outside of civilian oversight or command. Within the Tatmadaw the army is the dominant branch. The Tatmadaw is one of the most opaque militaries in the world, with little information on its structure or operations coming directly from the military itself.

4.4.2 Myanmar: Administrative Division

Myanmar is divided into Regions and States, a capital "Union Territory" and also has several Self-Administered Zones. Some of these administrative boundaries are divided into Districts which are further divided into Townships.

4.4.3 Myanmar: Security Forces

Tatmadaw/Armed Forces/Military

The Commander-in-Chief of the Tatmadaw is at the apex of the chain of command with a Deputy Commander-in-Chief of Defence Services directly below this position, who also concurrently serves as the head of the army.

Tatmadaw-Kyi/Army

As of 2009 the Commander-in-Chief of the Tatmadaw is at the apex of the chain of command, the military does not come under the command of civilian political leaders of Myanmar. Underneath the Commander-in-Chief is the Deputy Commander-in-Chief of Defence Services who concurrently serves as the head of the army. In the army's chain of command below the Deputy Commander-in-Chief of Defence Services is the General Staff Office (also referenced as the General Staff) which commands the six Bureaus of Special Operations (BSO). Each BSO commands one or more Regional Military Commands (RMC) which oversee army operations in one or more state, region or union territory. Below RMCs in the army hierarchy are Military Operations Commands (which generally command ten battalions), Regional Operations Commands (which generally command four battalions), and Tactical Operations Commands (which generally command three battalions). The main units of the army are Light Infantry Battalions and Infantry Battalions.

Light Infantry Divisions are regularly deployed for operations around the country and from 1990 to at least 2009 followed a separate chain of command, reporting directly to the Chief of Staff of the army (who heads the General Staff Office).

As of 2009 artillery formations were generally under a separate chain of command, with Artillery Battalions under the command of Artillery Divisions. The chain of command from Artillery Divisions to the rest of the military is currently unclear, however, they eventually fall under the Deputy Commander-in-Chief of Defence Services, who in turn is under the command of the Commander-in-Chief, as does the rest of the military of Myanmar.

4.4.4 Myanmar: Outstanding Areas for Further Research

- Investigating the command structure of other branches of the military as well as the police, border guards and other internal security forces.
- Expanding and deepening information on the command structure of artillery units.
- Detailing commanders of the various units of the security forces.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Myanmar.

4.5 Nigeria

4.5.1 Nigeria: Overview of Coverage

The Security Force Monitor's current dataset comprehensively covers the Nigerian armed forces and the Nigeria Police Force in the states of Abia, Adamawa, Akwa Ibom, Anambra, Enugu, Kano, Katsina, Lagos, Ogun, Plateau, Rivers and Yobe from roughly 2008 to 2018. Additional research (detailed below) will focus on other elements of the security forces of Nigeria.

4.5.2 Nigeria: General Background on Security Forces

Nigeria has security forces with different responsibilities for internal security. Crime fighting is the prime responsibility of the Nigeria Police Force. The State Security Service focuses on threats to national security. The Nigerian Armed Forces, comprising the Nigerian Air Force, Nigerian Army and Nigerian Navy, are also very active in internal security operations, particularly against Boko Haram. The Nigerian Army is generally the branch most closely involved in internal security operations. Security forces in Nigeria are generally national in character with the President of Nigeria as the commander-in-chief of the respective forces.

4.5.3 Nigeria: Administrative Division of Nigeria

Administratively, Nigeria has a federal structure with 36 states and a Federal Capital Territory (FCT). Each state and the FCT is broken up into Local Government Areas (LGA). There are 776 LGAs throughout the country.

4.5.4 Nigeria: Security Forces

Police

The Nigeria Police Force (NPF) is the national police force of Nigeria. The NPF is under control of the president and headed by the Inspector General of Police (IGP) who is appointed by the President. The command structure flows from the IGP at Force Headquarters through Zonal Police Commands, each of which oversee police operations in at least two states and/or the Federal Capital Territory (FCT). Each State and the FCT has a Police Command headed by a Commissioner of Police who commands police operations in the state or FCT. Each Police Command also has a Criminal Investigation Department and a Special Anti Robbery Squad (the command structure for Special Anti Robbery Squad units has changed multiple times). Police Commands are divided into several Police Area Commands which are under the command of the Police Command. Police Area Commands are further divided into Police Divisions, which usually headed by a Chief Superintendent of Police and often referred to by their title, Divisional Police Officer. Police Divisions can also be under the direct command of their respective Police Command. Police Divisions in turn command the smaller formation of Police Stations which in turn command Police Posts. The smallest formation of the NPF is the Village Police Post which can be commanded by either a Police Post or Police Division, depending on the structure of the police formations in that particular area.

Additionally, the Police Mobile Force (PMF, MOPOL or Mobile Police), are the riot police of the Nigerian Police Force, and report directly to Force Headquarters. The PMF is broken up into squadrons with each state and the FCT having at least one squadron. Department of State Security or State Security Service

The Department of State Security or State Security Service (DSS or SSS) is responsible for maintaining internal order and operates nationwide. The SSS is broken up into state commands headed by a Director of Security (commonly referred to as Director). The state commands are then under the command of the Director General of the SSS. The state commands may be further divided into branches covering each local government area of a state or the FCT.

Nigerian Armed Forces/Military

The President of Nigeria is the Commander-in-Chief of the Nigerian Armed Forces, and generally commands the forces through the Chief of Defense Staff who heads Defence Headquarters. The Minister of Defence is not in the chain of command, but provides administrative support to the military.

The Nigerian Armed Forces is broken up into independent branches - Nigerian Army (NA), Nigerian Navy (NN) and Nigerian Air Force (NAF). The army is the largest branch in terms of personnel and plays the major role in internal security. The head of each branch of the Armed Forces reports to the Chief of Defence Staff/Defence Headquarters.

Nigerian Army

The Army is under the command of the Chief of Army Staff who reports to the Chief of Defence Staff.

Operationally the Nigerian Army is organized into Divisions (a division is about 10,000 soldiers), the 1 Mechanised Division, 2 Mechanised Division, 3 Armoured Division, 81 Division, 82 Division, 7 Division, 8 Task Force Division and 6 Division. There is also an independent brigade, the Guards Brigade, charged with protecting the president and the Federal Capital Territory which reports directly to the President.

Each Division has several Brigades under its command and also has support units including and also has support units including an Engineering Division (or a Division of Engineers), a Signals Division (despite their name these formations are much smaller than 10,000 soldiers) and a Garrison unit. Each Brigade generally has three battalions or artillery regiments under its command as well as a Garrison unit. (The deployment of forces to the north east to battle Boko Haram has complicated the picture somewhat).

Nigerian Navy

The Navy is under the command of the Chief of Naval Staff who reports to the Chief of Defence Staff.

Operationally the Nigerian Navy is divided into the Western, Eastern and Central Naval Commands, each headed by a Flag Officer Commanding.

Nigerian Air Force

The Air Force under the command of the Chief of Air Staff who, in turn, reports to the Chief of Defence Staff.

Operationally, the Nigerian Air Force is divided into several operational commands - Tactical Air Command, Mobility Command, Training Command, Logistics Command - which report to the Chief of Air Staff. Joint Task Forces

Several Joint Task Forces (JTFs) operate and have operated throughout Nigeria. The mission profile and makeup of these JTFs have varied, though they generally include a police and army component. Most JTFs appear to have been commanded by army officers.

4.5.5 Nigeria: Outstanding Areas for Further Research

- Inclusion of additional details on units and commanders for Nigeria Police Force units in the Federal Capital Territory and the following states: Bauchi, Bayelsa, Benue, Borno, Cross River, Delta, Ebonyi, Edo, Ekiti, Gombe, Imo, Jigawa, Kaduna, Kebbi, Kogi, Kwara, Nasarawa, Niger, Ondo, Osun, Oyo, Sokoto, Taraba, Zamfara.
- Identifying additional details on individual units and personnel as needed to fill any gaps in the records of units and commanders of the armed forces of Nigeria during the timeframe of 2008 to 2018.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Nigeria.

4.6 Philippines

4.6.1 Philippines: Overview of Coverage

The Security Force Monitor's current dataset is a "snapshot" of the structure of the Philippine National Police as of January 2018. Additional research (detailed below) will focus on other elements of the security forces of the Philippines.

4.6.2 Philippines: Administrative Division

The Philippines is divided into regions, provinces, independent cities, municipalities and barangays. Security Forces of the Philippines

4.6.3 Philippines: Security Forces

Philippine National Police

The Philippine National Police (PNP) is national police force of the Philippines, established through the merging of precursor organizations and transfer of personnel and roles from other security agencies in December 1990.

The PNP is headed by a Chief of Police who is assisted by a Deputy Chief for Operations and a Deputy Chief for Administration. The basic hierarchical structure since the establishment of the PNP has been: regional offices commanded by a regional director, then provincial offices commanded by a provincial director (which can be subdivided into police districts commanded by a district director) and finally at the city or municipal level police stations commanded by a chief of police.

4.6.4 Philippines: Outstanding Areas for Further Research

- Expanding the command structure of the Philippine National Police through time.
- Detailing commanders of Philippine National Police across various units and branches.
- Identifying locations and areas of operations through time for units of the Philippine National Police.
- Building command hierarchy of the armed forces of the Philippines and identifying location and area of operations of various units.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of the Philippines.

4.7 Rwanda

4.7.1 Rwanda: Overview of Coverage

The Security Force Monitor's current dataset is a "snapshot" of the structure of the Rwanda National Police as of 2017. Additional research (detailed below) will focus on other elements of the security forces of Rwanda.

4.7.2 Rwanda: Administrative Division

Rwanda is divided into provinces, which are further subdivided into districts, sectors and cells.

4.7.3 Rwanda: Security Forces

Police

The Inspector General of Police commands the Rwanda National Police which is divided operationally into and Police Regions which are further divided into Police Districts, Police Stations, Police Posts.

4.7.4 Rwanda: Outstanding Areas for Further Research

- Expanding the command structure of the Rwanda National Police through time.
- Detailing commanders of Rwanda National Police across various units and branches.
- Identifying locations and areas of operations through time for units of the Rwanda National Police.
- Building command hierarchy of the armed forces of Rwanda and identifying location and area of operations of various units.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Rwanda.

4.8 Saudi Arabia

4.8.1 Saudi Arabia: Overview of Coverage

The Security Force Monitor's current dataset is a "snapshot" of the structure of the armed forces of Saudi Arabia as of 2009. Additional research (detailed below) will focus on other elements of the security forces of Saudi Arabia.

4.8.2 Saudi Arabia: Administrative Division

Saudi Arabia is divided into 13 regions with further subdivisions of governorates and then sub-governorates.

4.8.3 Saudi Arabia: Security Forces

Saudi Arabian National Guard

As of 2009 the King of Saudi Arabia exercised direct control over the Saudi Arabia National Guard (SANG). SANG is divided into two regional commands which command Brigades, as well as independent Brigades which report directly to SANG headquarters. Brigades commanded several Battalions. Additionally there were several independent battalions.

Military

As of 2009 the King of Saudi Arabia was the commander in chief of the armed forces. The chain of command went from the King through the Ministry of Defense and Aviation to the Chief of General Staff who commanded the four branches of the military: the Royal Saudi Land Forces (army), Royal Saudi Air Force, Royal Saudi Navy and Royal Saudi Air Defense Force.

Royal Saudi Air Force

As of 2009 the air force was divided into Wings which command Squadrons.

Royal Saudi Navy

As of 2009 the navy was divided into two fleets - the Western Fleet and Eastern Fleet.

4.8.4 Saudi Arabia: Outstanding Areas for Further Research

- Expanding the command structure of the armed forces and SANG through time.
- Detailing commanders of the various units of the armed forces and SANG through time.
- Identifying locations and areas of operations through time for units of the armed forces and SANG through time.
- Building command hierarchy of internal security forces of Saudi Arabia and identifying location and area of operations of various units.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Saudi Arabia.

4.9 Uganda

4.9.1 Uganda: Overview of Coverage

The Security Force Monitor's current dataset is a "snapshot" of the structure of the Uganda Police Force as of September 2016. Additional research (detailed below) will focus on other elements of the security forces of Uganda.

4.9.2 Uganda: Administrative Division

Uganda is divided into four regions which are further subdivided into 111 districts.

4.9.3 Uganda: Security Forces

Police

The Inspector General of Police commands the Uganda Police Force which is divided into Directorates at the headquarters level and operationally into and Police Regions which are further divided into Police Districts, Police Stations, Police Posts and Police Booths.

4.9.4 Uganda: Outstanding Areas for Further Research

- Expanding the command structure of the Uganda Police Force through time.
- Detailing commanders of the Uganda Police Force across various units and branches.
- Identifying locations and areas of operations through time of Uganda Police Force units.
- Building command hierarchy of the armed forces of Uganda and identifying location and area of operations of various units.
- Investigating other priorities as guided by partners concerned about the human rights practices of the security forces of Uganda.

What data does the Monitor collect?

5.1 Units, persons and incidents

Security Force Monitor researches and creates data about three things (or “entities”) related to security forces around the world:

- *Units* are official state or state-sanctioned organizations responsible for the internal or external security for a country, including the police, army, navy, air force and other security forces. Units refer to any any part of the hierarchy of a security force, ranging from a defense ministry with national jurisdiction, to a police unit based in a small town. Units can also be groupings of units such as “operations”, “joint task forces” or peacekeeping missions. The Monitor collects data about a unit’s name, aliases, bases and other physical infrastructure, geographical areas of operation and relationships with other units over time.
- *Persons* are natural persons who are affiliated with, or hold positions of command over a specific unit at a particular point in time. The Monitor creates a dossier for each person, which includes their name, aliases, rank, title, role and the different units which they are affiliated with. In addition, we use a format called *Persons Extra* to capture data about a person’s online and social media accounts, and media describing how a person looks and sounds
- *Incidents* are publicly-documented allegations of human rights violations committed by security forces. These include extrajudicial killings, rape, torture and other forms of violence. The Monitor does not make allegations itself, but rather compiles allegations made by governmental bodies, human rights organizations and other civil society actors. For each incident, the Monitor includes a description from the source, date(s), specific location(s), its perpetrators and the types of human rights violation alleged to have happened.

Every piece of data collected by the Monitor is individually sourced and each data point about *Persons* and *Units* is assigned a confidence score. The Research Handbook sections on *Sources* and *Data integrity measures* provide more guidance about these aspects of the data creation process.

Detailed guidance about the fields used by the Monitor to record data about *Units*, *Persons*, *Incidents* *Locations* is provided in the sections that follow.

5.2 Sample data entry sheets

Security Force Monitor uses databases, spreadsheets and other tools to capture and analyse the data described in this Research Handbook. Though the spreadsheet can get quite large and unwieldy, it remains an extremely powerful and effective way to capture and store data. To assist you with your research, here are the formats we use as a Google Sheet, and in Excel and OpenDocument formats:

- Sample data entry sheets [in Excel format](#).
- Sample data entry sheets [in Open Document format](#).
- Sample data entry sheets [as a Google Sheet](#).

Data integrity measures

The data we create is carefully collected from a variety of publicly available sources, generally online, which include laws of the country, government media and press releases, reports from civil society groups, and local and international news reports and many others. We comb through these sources and use the information we find to populate a set of fields about persons, units and incidents, and the relationships between them. The resulting data is a synthesis of information provided within a tapestry of different sources - over 7,000 at the time of writing. We collect data on sources themselves, including their titles, date of publication, online location - the data model for sources is documented in the *Sources* section of this handbook.

As part of our data creation method, we have implemented four powerful integrity measures that help ourselves and others users of the data interrogate and assess its quality: data point level evidencing; data point confidence scores; making data timebound; and, differentiation of unknown and unnamed units in the command chain. We'll now look at each in turn

6.1 Data point level evidencing

Data point level evidencing is the practice of recording the exact source we used to create a specific piece of data right alongside that piece of data.

For example, records about units cover dimensions like the unit's basic identity (Unit: Name, Unit: Country, Unit: Classification), its relationships with other units (Unit: Related Unit, Unit: Membership), its physical infrastructure (Unit: Base Name) and other dimensions. Data on units are structured in standard formats of over 60 possible fields. We may use hundreds of different sources to create a record about a single unit: however, the sources used to evidence the existence of a unit's base or area of operations may be different from those we use to evidence its participation in a peacekeeping mission. Further, the sources that show when a unit entered a particular location may be different from those that show when it left.

To overcome this challenge, we state what sources are used for each and every data point. This gives us the advantage of being able to quickly audit a data point; it also means we can see all the data points evidenced by a specific source, or a specific part of the source. This point is important: sources can have multiple access points, which we create to show that we used material from a particular page number or archive version of a source. The *Sources and Access Points* section of this Research Handbook provides more detail on this important concept.

This is quite an unusual way to structure data. In most row-based data capture systems that include data drawn from different sources, there may be a column that contains all the sources for that *row*, leaving the user of the data to guess which sources refer to which data point in the row:

Unit name	Start date	Sources
1 BAT	January	A,B,C,D,E
2 BAT	February	C,D,E,F,G

In our model, the sources for each data point are recorded alongside the relevant data point like this:

Unit name	Unit name sources	Start date	Start date sources
1 BAT	A,B	January	C,D,E
2 BAT	E,F,G	February	C,D,E

Implementing this system in practice is challenging. For simple data capture systems like spreadsheets, it means adding lots of additional columns to records the sources. If the data model has only a few columns, this isn't a problem; but for a model like ours with over 60 fields, it creates a very wide and cumbersome spreadsheet. Where the data capture system is a database with some control over the user interface, it still presents a challenge: we have overcome this in *WhoWasInCommand* by creating a special “source picker” which enables the user to search for a source, and then associate it with a data point.

6.2 Confidence scores

Confidence scores are measures of the degree to which the sources available to us agree on the content of a particular data point.

All the data points we create start with a confidence score of *Low* until a confluence of different sources indicate we should upgrade it to a designation of *Medium*. The gap between upgrading the confidence score of a data point from *Low* to *Medium* is smaller than when moving from *Medium* to *High*. This scoring system gives a useful indicator of a degree to which we can rely on a data point's accuracy.

Each data point (except those tied to an alleged incident) has a confidence score attached to it. The confidence scores only relate to the specific data point to which they are attached.

For instance, if a wide variety of sources agree that the *1 Division* is the name of an unit a confidence score of *High* would be assigned to this data point. However, if there is only one source for *One Division* as an alias, a confidence score of *Low* would be merited.

Confidence scores are determined first by agreement amongst sources about the overall structure and nature of the security forces. Sources for this type of information generally are laws of the country, government websites, and books. For example, if the law states that police force is divided into *Police Divisions* and *Police Stations* and a Monitor researcher comes across a source that references a particular *Police Division*, we would accept that source with *Low* confidence as this conforms with what other sources state about the structure of the police. Conversely, if a Monitor researcher came across a source that referenced a “Police Command Zone” they would need to do more research before publishing information on this potential unit, as “Police Command Zone” does not fit into what other sources state about the structure of the police. This could mean the other sources are incorrect, or that a change has occurred in the structure of the police force, or simply that this is a formation not referenced by the Monitor's other sources. Additional research would help clarify the situation.

6.3 Timebound Data

Answering the question “who was where when?” is central for investigations into allegations of human rights abuse(s). Because of this perhaps one of the most defining, and complicating, features of the Security Force Monitor’s data is that almost everything we research is connected to time including:

- Existence of units
- Parent relationships between units
- Location of units
- Areas of operation for units
- Membership/participation of units of in multi-unit operations
- Positions held by people

While attaching time to data points aids our mission to support human rights investigations and advocacy, it raises methodological challenges and questions such as:

- Why the Monitor would (or would not) connect two bits of data through time
- How the Monitor handles gaps in the public record
- Questions analysts run through while reviewing time based information

In an ideal world the Monitor would have a source from every day of the year stating where a unit was located or conducting operations. Barring that, having multiple sources regularly making statements like “since X date this unit has been based in this city” would be tremendously helpful. Unfortunately, neither scenario currently occurs, or is likely to occur in the near future, making it necessary to develop a robust way of thinking through time.

Broadly speaking the Security Force Monitor uses agreement among sources to build up details on security force units and individuals. Most of the Monitor’s sources, like government press releases and newspaper articles, can be used to link a value, such as the location of a unit, to a specific date (usually the date of publication). As we collect more sources we need to determine what agreement among sources means for time based values, like the location of a unit.

Example: the Monitor comes across Source A published on 1 July 2012 stating that the 1 Battalion is based in Lagos. If Source B published on 3 August 2012 also states that the 1 Battalion is based in Lagos we have a decision point about what claim we should make.

Using sources A and B we have two options which can be expressed in text:

1. Separate claims: “As of 1 July 2012 the 1 Battalion was based in Lagos and as of 3 August 2012 the 1 Battalion was based in Lagos, the Monitor does not know where the battalion was based between those two points in time.”
2. Contiguity claim: “From at least 1 July 2012 to at least 3 August 2012 the 1 Battalion was based in Lagos.”

Thus, whenever the Monitor gets a new source of information we have to decide whether to make a “separate” or “contiguity” claim. Based on the example of the 1 Battalion above the Monitor would run through a series of questions to determine which claim (if any) to make:

- In general, how do other battalions operate, are they sedentary, or highly mobile?
- How has the 1 Battalion acted in the past, has it been sedentary or highly mobile?
- Are there other sources disputing these claims (i.e. 1 Battalion being based solely in another city)?
- Are there any sources indicating the 1 Battalion was in Lagos in July and/or August as part of a “special”, “emergency” or otherwise temporary posting?
- Are there sources that indicate the 1 Battalion moved in between these two points of time and thus these should be treated as separate deployments to Lagos?

- Is there anything related to the 1 Battalion's parent or child units that may impact where it was based?
- Are there any other mitigating sources (i.e. major restructuring of the military, constitutional changes, etc.) which may impact the basing of the unit?
- Is more research needed before the Monitor can make any claim?

An argument could be the Monitor should always make “separate claims” as that would be more faithful to the sources. However, the result likely mean an almost incomprehensible amount of detail in the records of people and units, which would obscure when changes really did occur, for instance when a person changed positions or a unit ends operations in an area.

Perhaps the most important point is that it even though data points, like where a unit is based, can be continuous through time, it should never be assumed that those types of features remain consistent between two or more sources. Time is a constant challenge, but given that is a key element in identifying perpetrators of human rights abuses it is necessary to get it right.

6.4 Unknown vs. Unnamed Units

The Security Force Monitor regularly encounters ambiguity in sourcing which it has sought to highlight and resolve through the creation of units with “Unknown” or “Unnamed” in the `Unit: Name` field. The methodology behind these decisions is laid out below:

1. For “Unknown” units the Monitor will have sources for the overall hierarchical structure of a branch of the security forces, laying out how units should relate to one another up the chain of command. However, the Monitor often will have data on a unit which indicates where it should be in the chain of command, but does not have sourcing for a direct parent. In this case the Monitor creates a unit with “Unknown” in the `Unit: Name` and “Placeholder” for the `Unit: Classification` field.

Example: Multiple sources, including the laws of Nigeria, lay out that the chain of command for the Police goes from each state (and the Federal Capital Territory) having a single Police Command, under which are Police Area Commands and under Police Area Command are Police Divisions. For the Abayi Police Division the Monitor has sources placing it in Aba, Abia state, making it ultimately under the control of the Abia State Police Command, per the law. However, the Monitor does not have sources indicating which Police Area Command controls Abayi Police Division, thus the Monitor has created a unit called Unknown Police Area Command in Abia State which is the parent unit of Abayi Police Division. In turn Abia State Police Command is the parent of Unknown Police Area Command in Abia State, which connects Abayi Police Division to the wider police command structure.

For “Unnamed” units the Monitor will have sources that indicate an unit exists, but it does not give a proper name for that unit. In this case the Monitor will create an “Unnamed” unit and continue to update relevant fields related to this unit until such a time that a source is discovered to give it a proper name.

Example: There are several Regional Operations Commands in the army of Myanmar. Many of these have proper names, such as the 2 Regional Operations Command. Multiple sources reference a Regional Operations Command based in the city of Sittwe, identifying subordinate units, areas of operation and other information related to units. None of these sources, however, give this unit a numerical identifier. In order to capture information about this unit the Monitor named this unit Unnamed Regional Operations Command at Sittwe and will maintain that name until a source with a numerical identifier can be identified.

“Unknown” units exist solely to connect subordinate units to the wider command hierarchy. Since they are a creation of the Monitor they will not have sites, area of operations, memberships or persons attached to them. In contrast, “Unnamed” units have all of the related attributes of a unit, and can have persons attached to them. The only thing they lack is a proper name. As a final note, additional sourcing would change an “Unnamed” unit into a unit with a proper name, whereas additional sourcing could result in the deletion of an “Unknown” unit as an actual parent unit would be identified, removing the need for the “Unknown” unit to exist.

7.1 What are units?

Units are official state or state-sanctioned organizations responsible for the internal or external security for a country. They include police, army, navy, air force and other security forces, as well as those civilian institutions linked to security forces through the chain of command or other linkages. Units refer to any part of the hierarchy of a security force, ranging from a national defense ministry to a police post in a small town. Units can also be groupings of other units, including joint operations, task forces or peacekeeping missions.

Documented in this section of the handbook are field describing the following dimensions of units:

- their existence and identity;
- their position in the hierarchy of a security force;
- locations of physical infrastructure like posts, bases and camps;
- their areas of operations; and,
- memberships in joint operations or international peacekeeping missions.

A spreadsheet containing all the fields used by Security Force Monitor can be found in the section called [Sample data entry sheets](#).

7.2 Unit: Unique Identifier

Description

A unique 32 character code assigned to each unit in the dataset.

Type of field

Text and numbers

Example of use

a407be6a-28e6-4237-b4e9-307f27b1202e

Spreadsheet column name`unit:id:admin`**Shortcode**`u_id_a`**Sources**

No

Confidence

No

Guidance on use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs must be created easily using either installable or online tools, for example:

- Linux and OSX users: *uuidgen* command line tool.
- On the web: [UUID Generator](#).

The field is administrative, providing a reliable way to differentiate between different units. In earlier versions, Security Force Monitor used `unit:name` to do this role but this provided inefficient as the dataset grew.

The Staff Researcher must generate a unique identifying number for that unit and copy it into the field `unit:id:admin` for every row associated with that specific unit. This manual, copy-and-paste step is a potential source of error. The Staff Researcher must be careful never to re-use a UUID anywhere in this or other parts of the dataset.

Bulk updates made to WhoWasInCommand.com by spreadsheet import are based on the values in this field. For example, changes made in the row `a407be6a-28e6-4237-b4e9-307f27b1202e` in the spreadsheet will be applied to the unit with that UUID in WhoWasInCommand.

7.3 Unit: Research Owner

Description

Initials of Staff Researcher who first created the unit.

Type of field

Text

Example of use

TL, TW, MM

Spreadsheet column name`unit:owner:admin`**Shortcode**`u_own_a`**Sources**

No

Confidence

No

Guidance on use

This field is administrative and only used where data are created using a spreadsheets. It is a simple measure to help researchers keep track of records they have created, and may be used for arbitrary grouping and tagging of specific sets of rows if needed.

7.4 Unit: Research Status

Description

The place of a row of data in the research workflow.

Type of field

Text and numbers; controlled vocabulary.

Example of use

1, X

Spreadsheet column name

`unit:status:admin`

Shortcode

`u_sta_a`

Sources

No

Confidence

No

Guidance on use

Staff Researchers use this administrative field to indicate where a row of data stands in the research workflow between the first cut of a row of data, review by other researchers, and final readiness for publication. Values in this field are taken from the below controlled list:

- X: Row should be deleted.
- 0: First commit. This row of data has just been added and needs review.
- 1: Fixes needed. A reviewer has made comments that need to be addressed, which will be recorded in the `unit:comment:admin` field.
- 2: Fixes made. The owner of this data has addressed the reviewer's comments.
- 3: Clean. A final check has been made by a reviewer, and this row of data can be published.

This field is common to all main entities in the SFM data model.

7.5 Unit: Research Comments

Description

Observations specific to the process of reviewing data in this row, including fixes, refinements and other suggestions.

Type of field

Text

Example of use

Parent unit missing, Geography needs attention, Possible duplicate - merge?

Spreadsheet column name

unit:comments:admin

Shortcode

u_com_a

Sources

No

Confidence

No

Guidance on use

Staff Researchers use this field to exchange feedback about the data in the row. This may include changes needed to specific fields, references to sources that the owner of the row might look at, and other observations that can improve the quality of the data. Data in this field are not intended for publication. The comments field is common to all main entities in the SFM data model.

7.6 Unit: Name

Description

Canonical name of the unit.

Type of field

Text and numbers

Example of use

3 Armoured Division, Operations Command 3 Compañía de Infantería No Encuadrada, 7 Military

Spreadsheet column name

unit:name

Shortcode

u_n

Sources

Yes (unit:name:source, u_n_s)

Confidence

Yes (unit:name:confidence, u_n_c)

Guidance on use

As different sources will spell a unit's name in different ways the Security Force Monitor works to create a single canonical version of a unit's name based on sources and standardized to match the overall structure of and reporting about the security forces:

Example: Police Divisions are a class of police units in Nigeria. There are over 1000 units of this type nationwide. However, each individual Police Division may not have a citation for their formal name such as Lagos Police Division, but only have a citation (or numerous citations) for the less formal Lagos Division. The Monitor would list the name of the unit as Lagos Police Division with a note about the methodology behind that choice. The less formal Lagos Division name would be entered in the Unit: Aliases field (documented below).

Example: Army units of a country may follow a naming convention of a number and then name of unit: e.g. 3 Battalion or 25 Brigade. There may be a unit of which we only have citations for a variation on that: e.g. Fourth Battalion. In this case, the Monitor would list the name of the unit as 4 Battalion with a note about the methodology behind that choice. The Fourth Battalion name variant would be entered in the Aliases or alternative spellings field

Standardizations don't have specific sources, so we have created a specific source to use in these cases. Where a value in Unit: Name has been standardized, a source with the following title will be associated with it: "Name standardized in accordance with Security Force Monitor research".

Additionally, wherever possible, we will choose the most complete and complex version of a unit's name that can be evidenced by a source:

Example: 3 Armoured Division would be the entry, rather than the more informal 3 Division (which may have more citations).

The Monitor does not use ordinal indicators like 1st or 3rd in the name of an Unit. Instead these will be listed in the Unit: Other Names field (see below).

The Monitor uses the name in the official (local) language of the country where appropriate and/or possible.

Example: A unit in the Mexican Army would be called by its name in Spanish (10 Regimiento de Caballería Motorizado), rather than the English translation (10 Motorized Cavalry Regiment).

In an effort to standardize names across all countries, the Monitor generally uses Arabic numerals in the Unit: Name field. Where warranted by sources the Monitor will use Roman numerals like V or XI instead of 5 or 11 respectively.

In cases where multiple units have the same name the Monitor will distinguish them by adding unique identifying text based on the unit's Location or parent unit.

Example: There are multiple "Central Police Station" formations across Nigeria, some based in the same state. To better distinguish these are separate, distinct units the Monitor added information on where the units were located to the name field for instance Central Police Station (Awka, Anambra State) . In Myanmar there have been different units through time both the name Central Regional Military Command. To distinguish them the Monitor added information on when the unit came into existence to the name: Central Regional Military Command (post 199).

7.7 Unit: Other Names

Description

Other names for a unit, including aliases, alternative spellings and abbreviations.

Type of field

Text and numbers

Example of use

If 3 Armoured Division is used as the canonical Unit: Name of a unit, entries in the Unit: Other Names field may include 3 Div and Three Division.

Spreadsheet column name`unit:other_names`**Shortcode**`u_on`**Sources**`Yes (unit:other_names:source, u_on_s)`**Confidence**`Yes (unit:other_names:confidence, u_on_c)`**Guidance on use**

Different sources will spell a unit's name in different ways. We choose and record a canonical version of a unit's name in the `Unit: Name` field. All other spellings that we have found are treated as aliases and stored in this field.

Although we do not use ordinal indicators like 2nd or 10/o in the canonical name we choose for a unit, where a source uses an Ordinal we record it as an alias.

Example: We find a version of the unit name 3 Armoured Division that has an Ordinal indicator: 10/o. Regimiento de Caballería Motorizado. We would record this in the `Unit: Other Names` field.

7.8 Unit: Country

Description

ISO 3166 two letter code for the country from which a unit originates.

Type of field

Text; controlled vocabulary.

Example of use`mx, ug, ng`**Spreadsheet column name**`unit:country`**Shortcode**`u_c`**Sources**`Yes (unit:country:sources, u_c_s)`**Confidence**`Yes (unit:country:confidence, u_c_c)`**Guidance on use**

The `Unit: Country` field identifies the country this unit comes from. All entries in this field are two letter country codes taken from [ISO 3166](#).

For example, a unit from Nigeria would have the code `ng` and a unit from Brazil would have the code `br`

7.9 Unit: Classification

Description

Branch of the security services that the unit a part of or general descriptor for the unit.

Type of field

Text and numbers

Example of use

Army, Ejército, Police, Military, Military Police, Joint Operation

Spreadsheet column name

unit:classification

Shortcode

u_cl

Sources

Yes (unit:classification:sources,u_cl_s)

Confidence

Yes (unit:classification:confidence,u_cl_c)

Guidance on use

We use classifications to describe the basic nature of a specific unit and to assist investigations of potential linkages between reports of human rights abuses and the Security Force Monitor's dataset. As alleged perpetrators are usually identified in general terms of "soldiers" and "police" this field is important as a first step to understand potential linkages between units, persons and incidents. Unit: Classification values are useful supplements to Unit: Related Unit and Unit: Membership data we use to connect different units together.

The Unit: Classification field will contain a mix of standard terms and country-specific terms used to describe security force branches. In choosing terms to include in the Unit: Classification field we try to include terms that are used by country experts as well as those that are common terms. We also try to be economical and create as few, distinct terms as possible.

Example: a standard term we would apply to army units is Army. The equivalent in Mexico would be Ejército. We would capture both terms in the Unit: Classification field.

Units may have more than one classification, usually this will be when a unit can have "generic" and "specific" classifications.

Example: Units which are part of the army of a country may be coded as having a classification of Army as well as a classification of Military, whereas units which are part of the navy of a country would have classifications of Navy and Military. For both the army and navy unit their respective classifications are correct, the army and the navy are part of the military. Critically, this enables the Monitor or users of the Monitor's data to properly analyze allegations against "soldiers" and "members of the army" in the country. In the case of "soldiers" this analysis should include every unit with the classification of Military while if there is greater specificity of "members of the army" would mean excluding any unit with the classification of Navy and focusing only on those units with a classification of Army.

7.10 Unit: First Cited Date

Description

The earliest date that a source shows a unit exists, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

unit:first_cited_date

Shortcode

u_fcd

Sources

Yes (unit:first_cited_date:source, u_fcd_s)

Confidence

Yes (unit:first_cited_date:confidence, u_fcd_c)

Guidance on use

Along with the fields Unit: First Cited Date is also Unit's Start Date, Unit: Last Cited Date and Unit: Last Cited Date is Open-Ended the field Unit: First Cited Date provides data about the time period we can evidence a unit has existed.

The Unit: First Cited Date field contains a date that is either:

- The earliest date found in a source that specifically references a unit; or,
- The earliest date of publication of sources that make reference to a unit.

For example, if three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all refer to 1 Motorized Brigade, we will use 1 January 2012 as the Unit: First Cited Date. If the source published on 1 March 2012 refers to activity of 1 Motorized Brigade that occurred on 30 June 2011, we will use 30 June 2011 as the Unit: First Cited Date.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Unit: First Cited Date.

This field is clarified by the field Unit: First Cited Date is also Unit's Start Date which indicates whether the date included here is the actual date on which a unit was founded.

7.11 Unit: First Cited Date is also Unit's Start Date

Description

Indicates whether the value in Unit: First Cited Date is the actual date a unit was founded.

Type of field

Boolean

Example of use

Y, N

Spreadsheet column name

`unit:first_cited_date_start`

Shortcode

`u_fcds`

Sources

Yes. Inherits from Unit: First Cited Date (`unit:first_cited_date:source,u_fcd_s`).

Confidence

Yes. Inherits from Unit: First Cited Date (`unit:first_cited_date:confidence,u_fcd_c`).

Guidance on use

This is a clarifying field for Unit: First Cited Date:

- Y: used where a source references a unit and specifies the date that unit was created
- N: used in all other cases, indicating that the date is not a start date but the date of first citation.

7.12 Unit: Last Cited Date

Description

The most recent date for sourcing the unit's existence, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2013, 2013-12, 2013-12-28

Spreadsheet column name

`unit:last_cited_date`

Shortcode

`u_lcd`

Sources

Yes (`unit:last_cited_date:sources,u_lcd_s`)

Confidence

Yes (`unit:last_cited_date:confidence,u_lcd_c`)

Guidance on use

Along with the fields Unit: First Cited Date, Unit: First Cited Date is also Unit's Start Date and Unit: Last Cited Date is Open-Ended the field Unit: Last Cited Date provides data on the time period we can say a unit has existed.

The Unit: Last Cited Date field contains a date that is either:

- The latest date found in a source that specifically references a unit; or,
- The latest date of publication of sources that make reference to a unit.

For example, if three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all refer to 1 Motorized Brigade, we will use 1 March 2012 as the Unit: Last Cited Date. If the source published on 1 March 2012 refers to activity of 1 Motorized Brigade that occurred on 15 February 2012, we will use 15 February 2012 as the value in Unit: Last Cited Date.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Unit: Last Cited Date.

This field is clarified by Unit: Open-ended?, which indicates whether the date in Unit: Date last cited is the date a unit was disbanded.

7.13 Unit: Last Cited Date is Open-Ended

Description

Indicates whether the value in Unit: Last Cited Date the actual date on which a unit was disbanded or not.

Type of field

Single choice

Example of use

Y, N, E

Spreadsheet column name

unit:last_cited_date_open

Shortcode

u_lcdo

Sources

Yes. Inherits from Unit: Last Cited Date (unit:last_cited_date:source,u_lcd_s)

Confidence

Yes. Inherits from Unit: Last Cited Date (unit:last_cited_date:confidence,u_lcd_c)

Guidance on use

We use this field to clarify the meaning of the date entered in Unit: Last Cited Date. Depending on information available from sources, one of the below values should be chosen:

- E indicates the exact date this unit was disbanded, or ceases to exist.
- Y indicates that we assume this unit continues to exist.
- N indicates we do not assume that this unit continues to exist, but we do not have an exact end date.

7.14 Unit: Type of Relationship

Description

The type of relationship that exists between two units.

Type of field

Text and numbers; controlled vocabulary.

Spreadsheet column name

unit:relation_type

Shortcode

u_rut

Sources

Yes. Inherits from Unit: Related Unit (unit:related_unit:source,u_ru_s)

Confidence

Yes. Inherits from Unit: Related Units (unit:related_unit:confidence,u_ru_c)

Guidance on use

We use this field to define the nature of the relationship between the unit that is the subject of the row (as defined in Unit: Name) and the unit noted in Unit: Related Unit. The Staff Researcher must choose one of the two options below:

- child: the unit described in the row is immediately subordinate to the unit noted in Unit: Related Unit.
- member: the unit described in the row is a member of the unit noted in Unit: Related Unit.

The values included in this field are used to build the organizational structure of a branch of the security forces. This is discussed in more detail in the documentation below for the field Unit: Related Unit.

7.15 Unit: Related Unit Unique Identifier

Description

The UUID of the related unit.

Type of field

Text and numbers

Spreadsheet column name

unit:related_unit_id:admin

Shortcode

u_ruid_a

Sources

Yes. Inherits from Unit: Related Unit (unit:related_unit:source,u_ru_s)

Confidence

Yes. Inherits from Unit: Related Units (unit:related_unit:confidence,u_ru_c)

Guidance on use

All units referenced as relations in this cluster of “related units” fields must already have an original entry of their own. This value in this field should be the same as the value in unit:id:admin of the unit noted in unit:related_unit.

7.16 Unit: Related Unit

Description

The immediate superior or parent unit of the current unit, or the unit to which the current unit is a member.

Type of field

Text and numbers

Example of use

301 Artillery Regiment

Spreadsheet column name

unit:related_unit

Shortcode

u_ru

Sources

Yes (unit:related_unit:source,u_ru_s)

Confidence

Yes (unit:related_unit:confidence,u_ru_c)

Guidance on use

Unit: Related Unit and the accompanying cluster of fields is used to describe the relationships that exist between units. The SFM data model includes two types of relationship between units: “Hierarchic”, and “membership”.

“Hierarchic” relationships are time-bound parent-child relationships between two units that are part of the same branch of a security force. When the relationship is defined in this way, “Unit: Related Unit” is a synonym for “parent unit” in that it describes a unit that is “above” and distinct and separate from the present unit in some way. It also exercises authority over the “child” unit. The aggregated upwards relationships between units form organizational structured and command chains.

Over time, a unit may have different parents.

Example: In Nigeria the 112 Task Force Battalion had the parent of 7 Division Garrison between 12 November 2015 and 24 March 2016. The 112 Task Force Battalion was then under the 22 Task Force Brigade from 14 March 2017 to 26 October 2017.

Units can also have multiple parent relationships at the same time. For example, sources could indicate a unit has a formal legal parent unit while at the same time a new security body established by decree can also directly order the unit to carry out operations, establishing a second parent relationship.

“Membership” relationships indicate that a unit is member of or attached to internal/national joint operations, international peacekeeping operations, or other multi-unit efforts. Often when there is an “operation” or “joint task force”, it may not have have personnel of its own. Rather, personnel from a range of different units are assigned to it. Generally, these types of arrangements don’t put the operation “above” the unit in the organizational chart. There are two circumstances in which it is appropriate to define a relationship as a “Membership”. First, where multiple units operate as part of an “operation” focused on a specific mission. Second, where multiple units “lend” or otherwise deploy personnel who operate under the command of a force composition like a “Joint Task Force” or “Operation”, which usually has a commander of its own.

Example: soldiers from 1 Division are deployed to the northeast of Nigeria to operate under Operation BOYANA. 1 Division has a commander, but the soldiers as part of Operation BOYANA likely report to and take orders from the commander of Operation BOYANA. When the soldiers are done with their rotation, after several months, they return to their “home unit” 1 Division.

So while `Operation BOYANA` commands some soldiers who are part of `1 Division` it doesn't technically command all of the soldiers of `1 Division` (otherwise it would be the parent unit).

The type of relationship between units is determined by setting the value in `unit:relation_type`, which offers two options:

- `child` to define a hierarchic relationship. The unit specified in `unit:related_unit` is the parent of the unit in the present row.
- `members` to define a membership relationship. The unit specified in the present row is a member of the unit noted in `unit:related_unit`.

7.17 Unit: Related Unit Classification

Description

Type of relationships that exists between two units.

Type of field

Controlled vocabulary, single choice

Example of use

Command, Administrative, Informal

Spreadsheet column name

`unit:related_unit_class`

Shortcode

`u_ruc`

Sources

Yes (`unit:related_unit_class:source,u_ruc_s`)

Confidence

Yes (`unit:related_unit_class:confidence,u_ruc_c`)

Guidance on use

Units have a `Command` relationship when the related parent unit can order the unit to perform some operational activity. These cover both *de jure* and *de facto* relationships between units.

`Informal` relationships occur when there is a relationship outside of the legal or formal structure of security forces and where the exact nature of the relationship is unclear.

Example: Lagos state in Nigeria has a security council which is a meeting of the governor, and the top commanders of police and military units in the state. The security council should be considered its own unit. By law a governor of a state is not in the chain of command for the military or police forces, but the security council membership establishes a relationship between the units and meetings often result in new approaches to security being taken, such as different deployments of police. In this case, we could make the determination that an informal relationship exists between the security council and the police and military units.

`Administrative` relationships exist where a formal, non-command relationship exists between units, or where an administrative description is more accurate of the relationship between two units.

Example: By law the Ministry of Defence in Nigeria provides administrative support to the Nigerian Army, establishing a relationship we could classify as *Administrative*. The Standards Department of an Army Headquarters might be under the control of the Army Headquarters, meaning the Army Headquarters could order the Department to take some sort of action. This technically means the Department is under the “command” of the Headquarters, but the Monitor would describe this relationship as *Administrative* because the Department is not in the field conducting operations, it’s an administrative organ of the Army Headquarters.

7.18 Unit: Related Unit First Cited Date

Description

The earliest date that a source evidences a relationship between units, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column heading

unit:related_unit_first_cited_date

Shortcode

u_rufcd

Sources

Yes (unit:related_unit_first_cited_date:source,u_rufcd_s)

Confidence

Yes (unit:related_unit_first_cited_date:confidence,u_rufcd_c)

Guidance on use

Along with the fields *Unit: Unit Relationship Start Date*, *Unit: Related Unit Last Cited Date* and *Unit: Related Unit is Open-Ended* the field *Unit: Related Unit First Cited Date* provides data on the time period for which sources provide evidence that one unit is related to another as part of a hierarchy or as a membership.

The *Unit: Related Unit First Cited Date* field contains a date that is either:

- The earliest date found in a source that specifically references a relationship; or,
- The earliest date of publication of sources that make reference to a relationship.

For example, if three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all say that 3 Armoured Division became the parent of 1 Motorized Brigade, we will enter 1 January 2012 in *Unit: Related Unit First Cited Date*. If the source published on 1 March 2012 says that 3 Armoured Division became the parent of 1 Motorized Brigade on 30 June 2011, we will use 30 June 2011 as the *Unit: Related Unit First Cited Date*.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, such partial dates can be included in *Unit: Related Unit First Cited Date*.

This field is clarified by the field *Unit: Unit Relationship Start Date* (documented below) which indicates whether the date included here is the actual date on which a unit became related to another.

7.19 Unit: Unit Relationship Start Date

Description

Indicates whether the value in Unit: Related Unit First Cited Date is the actual date on which a unit became related to another, or the earliest date a source has referred to the relationship

Type of field

Boolean (Yes, No)

Example of use

Y, N

Spreadsheet column name

unit:related_unit_first_cited_date_start

Shortcode

u_rufcds

Sources

Yes. Inherits from Unit: Related Unit First Cited Date (unit:related_unit_first_cited_date:source, u_rufcd_s)

Confidence

Yes. Inherits from Unit: Related Unit First Cited Date (unit:related_unit_first_cited_date:confidence, u_rufcd_c)

Guidance on use

This is a clarifying field for Unit: Related Unit First Cited Date. Where a source references the hierarchic or membership relationship and specifies the date that the relationship began we will enter Y. In all other cases we will enter a value of N to indicate that the date is not a start date, but the date of first citation.

7.20 Unit: Related Unit Last Cited Date

Description

The latest date that a source evidences a hierarchic or membership relationship, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

unit:related_unit_last_cited_date

Shortcode

u_rulcd

Sources

Yes (unit:related_unit_last_cited_date:source, u_rulcd_s)

Confidence

Yes (unit:related_unit_last_cited_date:confidence,u_rulcd_c)

Guidance on use

Along with the fields Unit: Related Unit First Cited Date, Unit: Unit Relationship Start Date and Unit: Related Unit is Open-Ended the field Unit: Related Unit Last Cited Date provides data on the time period we can evidence that one unit is related to another.

The Unit: Related Unit Last Cited Date field contains a date that is either:

- The latest date found in a source that specifically references a relationship; or,
- The latest date of publication of sources that make reference to a relationship.

Example: Three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all state that the 1 Motorized Brigade is under the 3 Armoured Division (which evidences a parent relationship), we will enter 1 March 2012 in Unit: Related Unit Last Cited Date.

Example: A source published on 23 July 2017 describes actions undertaken by the 1 Motorized Brigade is under the 3 Armoured Division during riots in 2009, and another source published on 8 June 2008 states that the 1 Motorized Brigade is under the 3 Armoured Division, we would enter 2009 in Unit: Related Unit Last Cited Date.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Unit: Related Unit Last Cited Date

Example: A source published on 23 July 2017 describes actions undertaken by the 1 Motorized Brigade is under the 3 Armoured Division during riots in 2009, and another source published on 8 June 2008 states that the 1 Motorized Brigade is under the 3 Armoured Division, we would enter 2009 in Unit: Related Unit Last Cited Date.

This field is clarified by the field Unit: Related Unit is Open-Ended, which indicates whether the date included here is the actual date on which a unit stopped being related to another.

7.21 Unit: Related Unit is Open-Ended

Description

Indicates whether or not the value in Unit: Related Unit Last Cited Date is the actual date on which the hierarchic or membership relationship ended.

Type of field

Single choice (Y, N, E)

Example of use

Y, N, E

Spreadsheet column name

unit:related_unit_open

Shortcode

u_ruo

Sources

Yes. Inherits from Unit: Related Unit Last Cited Date (unit:related_unit_last_cited_date:source, u_rulcd_s)

Confidence

Yes. Inherits from Unit: `Related Unit Last Cited Date` (unit:related_unit_last_cited_date:confidence_u_rulcd_c)

Guidance on use

We use this field to clarify the meaning of the date entered in Unit: `Related Unit Last Cited Date One` of the below values should be chosen:

- E indicates the exact date one unit stopped being related to another.
- Y indicates that we assume this relationship continues to exist.
- N indicates we do not assume that this relationship continues to exist, but we do not have an exact end date.

7.22 Unit: Location Type

Description

The type of Location of a unit.

Type of field

Text and numbers; controlled vocabulary.

Spreadsheet column name

unit:location_type

Shortcode

u_loct

Sources

Yes. Inherits from Unit: `Location` (unit:location:source,u_loc_s)

Confidence

Yes. Inherits from Unit: `Location` (unit:location:confidence,u_loc_c)

Guidance on use

This field defines the relationship between a unit and a Location. The Staff Researcher must choose one of the two options below:

- `site`: the Location in `unit:location` describes a “site”, such as a settlement or specific point, at which the unit has physical infrastructure like a station, camp, base, office or other facility.
- `ao`: the Location in `unit:location` describes an area, such as an administrative area, where the unit is known to have conducted operations or has territorial jurisdiction.

The type of Location may be different from the way that the Location is described. For example, a small geographic area like a suburb is a *geometric area* but it could be used to describe a “site” for a unit. This is why *Locations* are defined independently of their relationship to Units and Incidents.

7.23 Unit: Base Name

Description

A base is a distinctively named building or complex - like a barracks or camp - where the unit is located.

Type of field

Text and numbers

Example of use

Leopard Base, Giwa Barracks, Bonny Camp

Spreadsheet column name

`unit:base_name``

Shortcode

`u_bn`

Sources

Yes (`unit:base_name:source, u_bn_s`)

Confidence

Yes (`unit:base_name:confidence, u_bn_c`)

Guidance on use

The `Unit: Base Name` field adds unit-specific context about a Location. This field is used to record data about units that are located in a distinctively-named building or complex.

For example, 3 Battalion in Nigeria is cited as being based in the Lubanga Barracks in Enugu, Enugu State, Nigeria.

This field should not be used for anything that matches the name or alias of a unit. For example, North Sector Police Station should not be put in this field if the name of the unit is North Sector Police Station.

7.24 Unit: Location

Description

Name of a Location where the unit has a “site” or “area of operations”.

Type of field

Text and numbers; linked to `location:humane_id:admin`

Example of use

Ikorodu (osm, point) 93dcc4a8-8335-4a21-8372-a151c4972c54

Spreadsheet column name

`unit:location`

Shortcode

`u_loc`

Sources

Yes (`unit:location:source, u_loc_s`)

Confidence

Yes (`unit:location:confidence, u_loc_c`)

Guidance on use

This field is used to store information about a [Locations](#) at which the unit has infrastructure, or as operated. The value included in this field must be taken from `location:humane_id_admin`. For further guidance on the creation, management and use of Locations visit the [Locations](#) documentation.

7.25 Unit: Location First Cited Date

Description

This field captures the earliest citation date for the location of a site or area of operations, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

`unit:location_first_cited_date`

Shortcode

`u_sfcd`

Sources

Yes (`unit:location_first_cited_date:source,u_locfcd_s`)

Confidence

Yes (`unit:location_first_cited_date:confidence,u_locfcd_c`)

Guidance on use

Along with the fields `Unit: Location was founded on First Cited Date`, `Unit: Location Last Cited Date` and `Unit: Location Last Cited Date is Open-Ended` the field `Unit: Location First Cited Date` provides data on the time period at which a unit was sited or operated in a Location.

The `Unit: Location First Cited Date` field contains a date that is either:

- The earliest date found in any source that references the value contained `Unit: Location`; or,
- The earliest date of publication of any source that references the value contained in `Unit: Location`.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in `Unit: Location First Cited Date`.

This field is clarified by the field `Unit: Location was Founded on First Cited Date` which indicates whether the date included here is the actual date on which a unit site was founded.

7.26 Unit: Location was Founded on First Cited Date

Description

Indicates whether or not the value in `Unit: Location First Cited Date` the actual date on which a unit site or area of operations was founded.

Type of field

Boolean (Yes, No)

Example of use

Y, N

Spreadsheet column name

`unit:location_first_cited_date_founding`

Shortcode

`u_sfcd_f`

Sources

Yes. Inherits from Unit: `Location First Cited Date(unit:location_first_cited_date:source, u_locfcd_s)`

Confidence

Yes. Inherits from Unit: `Location First Cited Date(unit:location_first_cited_date:confidence, u_locfcd_c)`

Guidance on use

This is a clarifying field for Unit: `Location First Cited Date`. There are two options for use in this field:

- Y: Where a source references a unit site and specifies the date that unit site was founded.
- N: In all other cases, indicate that the date is not a start date, but the date of first citation.

7.27 Unit: Location Last Cited Date

Description

This field is for the latest citation for the location of a unit site or area of operations, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

`unit:location_last_cited_date`

Shortcode

`u_locld`

Sources

Yes (unit:location_last_cited_date:source, u_locld_s)

Confidence

Yes (unit:location_last_cited_date:confidence, u_locld_c)

Guidance on use

Along with the fields `Unit: Location First Cited Date`, `Unit: Location was founded on First Cited Date` and `Unit: Location Last Cited Date is Open-Ended` the field `Unit: Location Last Cited Date` provides data on the time period that a unit was sited or operated at a Location.

The `Unit: Location Last Cited Date` field contains a date that is either:

- The latest date found in any source that references the value contained in `Unit: Location`; or,
- The latest date of publication of any source that references the value contained in `Unit: Location`.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in `Unit: Location Last Cited Date`.

This field is clarified by the field `Unit: Location Last Cited Date is Open-Ended` which indicates whether the date included here is the actual date on which a unit was no longer sited or operating in the Location.

7.28 Unit: Location Last Cited Date is Open-Ended

Description

Indicates whether the value in `Unit: Location Last Cited Date` is the actual date on which a unit ceased to be sited or operate in a Location, the latest date a source has referred to a unit's Location, and whether can we assume this unit continues to be sited or operate at this Location.

Type of field

Single choice (Y, N, E)

Example of use

Y, N, E

Spreadsheet column name

`unit:location_open`

Shortcode

`u_loclcd_o`

Sources

Yes. Inherits from `Unit: Location Last Cited Date` (`unit:location_last_cited_date:source`, `u_loclcd_s`)

Confidence

Yes. Inherits from `Unit: Location Last Cited Date` (`unit:location_last_cited_date:confidence`, `u_loclcd_c`)

Guidance on use

We use this field to clarify the meaning of the date entered in `Unit: Location Last Cited Date`. In entering a value for this field we use a variety of factors including: the history of basing and operations for the unit, the overall structure and nature of the security forces, and the frequency of movement of similar units.

The values that can be entered in this field are restricted to the below:

- E: indicates the exact date this unit ceased to be sited or operate in this Location.
- Y: indicates that we assume this unit continues to be sited or operate in this Location,
- N: indicates we do not assume that this unit continues to be sited or operate in this Location, but we do not have an exact end date.

7.29 Unit: Notes

Description

Analysis, commentary and notes about the unit that do not fit into the data structure.

Type of field

Text and numbers

Example of use

In March 1990 the previous Central Regional Military Command based in Taungoo was renamed Southern Regional Military Command, the previous Northwestern Regional Military Command based in Mandalay was renamed as the Central Regional Military Command and a new Northwestern Regional Military Command was created in Monywa.

Spreadsheet column name

unit:notes:admin

Shortcode

u_n_a

Sources

No

Confidence

No

Guidance on use

We use this field to record information about the unit that is likely to provide useful context, additional information that does not fit into the data structure, and notes about how decisions were made about which data to include. Any sources used in the note should be created as *Sources* and its access point UUID included (from `source:access_point_id:admin`) included directly in the field.

8.1 What are persons?

Persons are natural persons who are affiliated with, or hold positions of command over a specific unit at a particular point in time.

The fields in the “Persons” data capture format are used to record basic details about a person’s identity, along with their career within a branch of the security force. Using these fields we can capture a persons rank, role and title in one or numerous differe units and see how it has changed over time.

This data capture format is supplemented by the “Persons Extra” format, which enables the capture of other biographical details (like their date of birth, and then they may have died), their social media accounts, and media that provide information about how a person looks and sounds.

A spreadsheet containing all the fields used by Security Force Monitor can be found in the section called [Sample data entry sheets](#).

8.2 Person: Unique Identier

Description

A unique 32 character code assigned to each person in the dataset.

Type of field

Text and numbers

Example of use

a848de4e-eb eb-49d6-9099-7e68ca3b57fc

Spreadsheet column name

person:id:admin

Shortcode

p_id_a

Sources

No

Confidence

No

Guidance on use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs can be created easily using either installable or online tools, for example:

- Linux and OSX users: *uuidgen* command line tool.
- On the web: [UUID Generator](#).

The field is administrative, providing a reliable way to differentiate between different persons. In earlier versions, Security Force Monitor used `person:name` to do this role but this provided inefficient as the dataset grew.

When a new person is created directly in WhoWasInCommand, the platform automatically creates a UUID for that person and stores it in this field. If a new person is created in a spreadsheet, the Staff Researcher must generate a unique identifying number for that person and copy it into the field `person:id:admin` for every row associated with that specific person. This manual, copy-and-paste step is a potential source of error and the Staff Researcher must be careful not to re-use a UUID.

Bulk updates made to WhoWasInCommand.com by spreadsheet import are based on the values in this field. For example, changes made in the row `a407be6a-28e6-4237-b4e9-307f27b1202e` in the spreadsheet will be applied to the person with that UUID in WhoWasInCommand.

8.3 Person: Research Owner

Initials of Staff Researcher who first created the person.

Type of field

Text

Example of use

TL, TW, MM

Spreadsheet column name

`person:owner:admin`

Shortcode

u_own_a

Sources

No

Confidence

No

Guidance on use

This field is administrative and only used where data are created using a spreadsheets. It is a simple measure to help researchers keep track of records they have created. These data are not imported into WhoWasInCommand. Instead,

WhoWasInCommand keeps a record of the changes (edits, new records, deletions) by the name of the system user who made them.

8.4 Person: Research Status

Description

The place of a row of data in the research workflow.

Type of field

Number range from 0 to 3

Example of use

1

Spreadsheet column name

`person:status:admin`

Shortcode

`u_sta_a`

Sources

No

Confidence

No

Guidance on use

This administrative field is only used in spreadsheets. Staff Researchers use this field to indicate where a row of data stands in the research workflow between the first cut of a row of data, review by other researchers, and final readiness for publication. Values in this field are taken from the below controlled list:

- 0: First commit. This row of data has just been added and needs review.
- 1: Fixes needed. A reviewer has made comments that need to be addressed, which will be recorded in the `person:comment:admin` field.
- 2: Fixes made. The owner of this data has addressed the reviewer's comments.
- 3: Clean. A final check has been made by a reviewer, and this row of data can be published.

Data created and managed in WhoWasInCommand does not use this mechanism. At the time of writing, a simple review system is being implemented in WhoWasInCommand.

8.5 Person: Research Comments

Description

Observations specific to the process of reviewing data in this row, including fixes, refinements and other suggestions.

Type of field

Text

Example of use

Parent person missing, Possible duplicate - merge?

Spreadsheet column name

person:comments:admin

Shortcode

u_com_a

Sources

No

Confidence

No

Guidance on use

This is an administrative field specific to data created in spreadsheets. Staff Researchers use it to pass on feedback about the data in the row. This may include changes needed to specific fields, references to sources that the owner of the row might look at, and other observations that can improve the quality of the data. Data in this field are not intended for publication.

8.6 Person: Name

Description

Full name of the person, including given, patronym and surnames.

Type of field

Text and numbers

Example of use

Magaji Musa Majia'a

Spreadsheet column name

person:name

Shortcode

p_n

Sources

Yes (person:name:source, p_n_s)

Confidence

Yes (person:name:confidence, p_n_c)

Guidance on use

Different sources will spell the name of a person in different ways, so we choose a name to be a canonical entry for that person. Whenever possible, the canonical entry will contain the most complicated or complete version of a person's name, even if it has the smallest number of citations. For example Magaji Musa Majia'a will be used instead of Magaji Majiaa. Other names will be placed in the Person: Other Names field (documented below). Titles, roles, honorifics and other attributes that are more correctly linked to a person's posting in a unit are recorded in fields like Person: Posting Rank, Person: Posting Role or Person: Posting Title.

8.7 Person: Other Names

Description

Other names used to identify a person.

Type of field

Text and numbers, free entry

Example of use

Virgilio Daniel Méndez Bazan, Virgilio Daniel Mendez Bazán

Spreadsheet column name

person:other_names

Shortcode

p_on

Sources

Yes (person:name:source, p_on_s)

Confidence

Yes (person:other_names:confidence, p_on_c)

Guidance on use

Different sources will spell a person's name in different ways. We choose and record a canonical version of a person's name in the `Person: Name` field. All other spellings that we have found are treated as aliases and stored in this field. This field may contain multiple values, which will be separated by a semi-colon. Titles, roles, honorifics and other attributes that are more correctly linked to a person's posting in a unit are recorded in fields like `Person: Posting Rank`, `Person: Posting Role` or `Person: Posting Title`.

8.8 Person: Country

Description

Country where a unit that a person is a member of is located.

Type of field

Text, controlled vocabulary

Example of use

mx

Spreadsheet column name

person:country

Shortcode

p_c

Sources

Yes (person:country:source, p_c_s), but only in WhoWasInCommand and not spreadsheets.

Confidence

Yes (`person:country:confidence, p_c_c`), but only in WhoWasInCommand and not spreadsheets.

Guidance on use

Values for this field are chosen from the list of ISO 3166-1 alpha-2 codes, which can be found ([on the ISO website](#) and on [Wikipedia](#)). This field does not denote the citizenship or country of origin of a person. Rather, it denotes where a unit they are a member of is located. For example, if 1 Batallón de Infantería is located in Juarez, Mexico, the unit will be assigned a value of `mx` in the field `Unit: Country`. Any person who is a member of that unit will be assigned a value of `mx` in the field `Person: Country` as well. A person may have multiple entries for `Person: Country` where our research shows they or a unit they are a member of is deployed to different countries.

8.9 Person:: Unique Identifier of Posting Unit

Description

A unique 32 character code assigned to each unit in the dataset, as already recorded in the `unit:id:admin` field of the [Units](#) sheet.

Type of field

Text and numbers; linked to `unit:id:admin`

Example of use

`a848de4e-eb9b-49d6-9099-7e68ca3b57fc`

Spreadsheet column name

`person:posting_unit_id:admin`

Shortcode

`p_puid_a`

Sources

Yes. Inherits from `Person: Name of Posting Unit (person:posting:source, p_pn_s)`

Confidence

Yes. Inherits from `Person: Name of Posting Unit (person:posting:confidence, p_pn_c)`

Guidance on use

This field is used to store the UUID of the unit to which the person is posted, and which is named in `person:posting_unit_name`. The unit must already have an entry in the [Units](#) dataset. The value must be identical to that in `unit:id:admin`.

8.10 Person: Name of Posting Unit

Description

The unit that the person is a member of.

Type of field

Text and numbers, controlled vocabulary

Example of use

`35 Batallón de Infantería`

Spreadsheet column name

person:posting_unit_name

Shortcode

p_pn

Sources

Yes (person:posting:source, p_pn_s)

Confidence

Yes (person:posting:confidence, p_pn_c)

Guidance on use

Values in this field correspond with names of units that already exist in the dataset (recording in the field Unit : Name. A person can have multiple postings to the same unit. These are triggered when there is a change to their entries for Person: Posting Rank, Person: Posting Title or Person: Posting Role with respect to the unit. An example of this is where a person is promoted. Another case where a person can have multiple posting of the same unit is where research indicates there are clear start or end dates to a posting. An example of where this might occur is if a person does multiple “tours” in a particular unit.

8.11 Person: Posting Role

Description

The role a person plays in the unit that is not evident from entries in Person: Posting Title or Person: Posting Rank.

Type of field

Text and numbers, controlled vocabulary

Example of use

Commander

Spreadsheet column name

person:posting_role

Shortcode

p_pro

Sources

Yes (person:posting_role:source, p_pro_s)

Confidence

Yes (person:posting_role:confidence, p_pro_c)

Guidance on use

The most common value we record in Person: Posting Role is Commander.

There are a variety of other roles a person can have including Second in Command, Chief of Staff along with other less common entries. They will vary between countries.

As a special note, heads of academic or other security force institutions will sometimes be referred to as the `Commandant`. In these cases, `Commandant` should be recorded in the `Title` field, and their role should be recorded as `Commander`.

If a person is referred to as “the head”, “chief” or some other variation indicating that they are in charge of a unit, they should be regarded as the `Commander` for the purposes of entering a value in `Person: Posting Role`.

8.12 Person: Posting Title

Description

A title held by a person that is separate from their rank or role.

Type of field

Text and numbers, free entry

Example of use

General Officer Commanding, Jefe Del Estado Mayor

Spreadsheet column name

`person:posting_title`

Shortcode

`p_pt`

Sources

Yes (`person:posting_title:source,p_pt_s`)

Confidence

Yes (`person:posting_title:confidence,p_pt_c`)

Guidance on use

The range of titles will vary from country to country. For example, commanders of army divisions in Nigeria, who usually hold the rank of `Major General` also hold the title of `General Officer Commanding`.

8.13 Person: Posting Rank

Description

The official position of a person in the hierarchy of a security force.

Type of field

Text and numbers, free entry

Example of use

General de División, Teniente Coronel, Air Vice Marshal

Spreadsheet column name

`person:posting_rank`

Shortcode

`p_pr`

Sources

Yes (person:posting_rank:source,p_pr_s)

Confidence

Yes (person:posting_rank:confidence,p_pr_c)

Guidance on use

We remove any dashes that are contained in Person: Posting Rank values.

For example, we would enter Brigadier General rather than Brigadier-General.

8.14 Person: Posting First Cited Date

Description

The earliest date a source evidences a relationship between a person and a unit, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

person:posting_first_cited_date

Shortcode

p_pfcd

Sources

Yes (person:posting_first_cited_date:source,p_pfcd_s)

Confidence

Yes (person:posting_first_cited_date:confidence,p_pfcd_c)

Guidance on use

Along with the fields Person: Posting First Cited Date is Start Date, Person: Posting Last Cited Date and Person: Posting Last Cited Date is End Date this field provides data about the time period over which we can evidence a person's relationships to a unit.

The Person: Posting First Cited Date field contains a date that is either:

- The earliest date found in the content of a source that specifically references the relationship between a person and a unit; or,
- The earliest date of publication of sources that makes reference to the relationship between a person and a unit.

For example, if three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all refer to this person as a commander, we will use 1 January 2012 as the value in Person: Posting First Cited Date. If the source published on 1 March 2012 refers to this person as a commander on the date of 30 June 2011, we will use 30 June 2011 as the value in Person: Posting First Cited Date.

The values for `Person: Posting Title`, `Person: Posting Role` and `Person: Posting Rank` held by a person are assumed to continue until a source indicates a change in any of those values. If the person's role, title or rank changes a new entry will need to be created to document that change. This new entry will have updated values for `Person: Posting First Cited Date` and related date fields.

For example, if a source indicates that Major General Jack Johnson is the commander of 1 Division as of 2007-08-20 all of the relevant fields would be entered based on that source. If another source states that Jack Johnson retired from the 1 Division on 2008-01-10 the last citation for Jack Johnson's affiliation would be 2008-01-10. However, this would also assume that Jack Johnson continued to have the Role of Commander and the Rank of Major General from 2007-08-20 until 2008-01-10.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in `Person: Posting First Cited Date`.

This field is clarified by the field `Person: Posting First Cited Date is Start Date` which indicates whether the date included here is the actual date on which the relationship between a person and a unit started.

8.15 Person: Posting First Cited Date is Start Date

Description

Indicates whether the value in `Person: Posting First Cited Date` is the actual date on which a person became a member of this unit, or the earliest date a source has referred to the relationship.

Type of field

Boolean

Example of use

Y, N

Spreadsheet column name

`person:posting_first_cited_date_start`

Shortcode

`p_pfcds`

Sources

Yes. Inherits from `Person: Posting First Cited Date` (`person:posting_first_cited_date:source, p_pfc_d_s`)

Confidence

Yes. Inherits from `Person: Posting First Cited Date` (`person:posting_first_cited_date:confidence, p_pfc_d_c`)

Guidance on use

This is a clarifying field for `Person: Posting First Cited Date` and has two options:

- Y: Where the content of the source has indicated the exact date that a relationship between a person and a unit began
- N: In all other cases we will enter a value of N to indicate that the date is not a start date, but the date of first citation.

8.16 Person: Context for Posting Start Date

Description

Additional information explaining why we are able to be specific about the start date of a person's specific posting to a unit.

Type of field

Text

Example of use

Person was promoted on this date, Person retired from the army on this date

Spreadsheet column name

person:posting_first_cited_date_start_context

Shortcode

p_pfcpsc

Sources

Yes (person:posting_first_cited_date_start_context:source, p_pfcpsc_s)

Confidence

Yes (person:posting_first_cited_date_start_context:confidence, p_pfcpsc_c)

Guidance on use

This field is not currently in use in spreadsheets or WhoWasInCommand.

This is a clarifying field for the Person: Posting First Cited Date is Start Date, and enables us to capture the reasons that persons move between units. The data in this field should be a simple statement summarising the reason described in the source.

8.17 Person: Posting Last Cited Date

Description

The latest date a source evidences a relationship between a person and a unit, either through direct reference in the source or by the date of its publication.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

person:posting_last_cited_date

Shortcode

p_plcd

Sources

Yes (person:posting_last_cited_date:source, p_plcd_s)

Confidence

Yes (person:posting_last_cited_date:confidence,p_plcd_c)

Guidance on use

Along with the fields Person: Posting First Cited Date, Person: First Cited Date is Start Date, and Person: Posting Last Cited Date is End Date the field Person: Posting Last Cited Date provides data about the time period over which we can evidence a person's relationships to a unit.

The Person: Posting Last Cited Date field contains a date that is either:

- The latest date found in the content of a source that specifically references the relationship between a person and a unit; or,
- The latest date of publication of sources that makes reference to the relationship between a person and a unit.

For example, if three sources published on 1 January 2012, 1 February 2012 and 1 March 2012 all refer to this person as a commander, we will use 1 March 2012 as the value in Person: Posting Last Cited Date. If the source published on 1 March 2012 refers to this person as a commander on the date of 14 February 2011, we will use 14 February 2011 as the value in Person: Posting Last Cited Date.

The values for Person: Posting Title, Person: Posting Role and Person: Posting Rank held by a person are assumed to continue until a source indicates a change in any of those values. If the person's role, title or rank changes a new entry will need to be created to document that change. This new entry will have updated values for Person: Posting Last Cited Date and related date fields.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included Person: Posting Last Cited Date.

This field is clarified by the field Person: Posting Last Cited Date is End Date which indicates whether the date included here is the actual date on which the relationship between a person and a unit ended.

8.18 Person: Posting Last Cited Date is End Date

Description

This field indicates whether the value in Person : Posting Last Cited Date is the actual end date on which the person ceased to be a member of this unit or if it is only the date last cited for that relationship.

Type of field

Boolean

Example of use

Y, N

Spreadsheet column name

person:posting_last_cited_date_end

Shortcode

p_plcde

Sources

Yes. Inherits from Person: Posting Last Cited Date (person:posting_last_cited_date:source, p_plcd_s)

Confidence

Yes. Inherits from Person: Posting Last Cited Date (person:posting_last_cited_date:confidence, p_plcd_c)

Guidance on use

This is a clarifying field for Person : Posting Last Cited Date. One of the below values should be chosen:

- Y indicates that the content of the source is the exact date that a relationship between a person and a unit ended.
- N indicates that the date is not an exact end date, but the date of last citation.

8.19 Person: Context for Posting End Date

Description

Additional information explaining why we are able to be specific about the end date of a person's specific posting to a unit.

Type of field

Text

Example of use

Person was promoted on this date, Person retired from the army on this date

Spreadsheet column name

person:posting_first_cited_date_end_context

Shortcode

p_pfcdec

Sources

Yes (person:posting_first_cited_date_end_context:source, p_pfcdec_s)

Confidence

Yes (person:posting_first_cited_date_end_context:confidence, p_pfcdec_c)

Guidance on use

This field is not currently in use in spreadsheets or WhoWasInCommand.

This is a clarifying field for the Person: Posting Last Cited Date is Date, and enables us to capture the reasons that persons move between units. The data in this field should be a simple statement summarising the reason described in the source.

8.20 Person: Notes

Description

Analysis, commentary and notes about the person that do not fit into the data structure.

Type of field

Text and numbers

Example of use

Trained in logisitics at Fort Lackland, Texas and the air force base of Wright Patterson, Ohio.

Spreadsheet column name

person:notes:admin

Shortcode

p_n_a

Sources

No

Confidence

No

Guidance on use

We use this field to record information about the person that is likely to provide useful context, additional information that does not fit into the data structure, and notes about how decisions were made about which data to include. Any sources used in the note should be created as *Sources* and the access point UUID (as stored in `source:access_point_id:admin`) should be included directly in the note.

CHAPTER 9

Persons Extra

The “Persons Extra” data capture format is used to extend the data in the *Persons* format to cover a person’s social media and other online accounts, official webpages, and media materials containing information about how the person looks and sounds.

It also serves the purpose of grouping resources that are *ipso facto* - resources that are valuable in themselves, and not only as sources for other data points. This provides the Staff Analyst with a collection of audiovisual media resources that can be used to identify and further research the person.

A spreadsheet containing all the fields used by Security Force Monitor can be found in the section called *Sample data entry sheets*.

9.1 Person Extra: Name

Description

Full name of the person, including given, patronym and surnames, as already recorded in the `person:name` field of the *Persons* sheet.

Type of field

Text and numbers

Example of use

Magaji Musa Majia'a

Spreadsheet column name

`person_extra:name`

Shortcode

`px_n`

Sources

No.

Confidence

No.

Guidance on use

This field is used to store the name of the person about whom extra information is being entered. The person must already have an entry in the *Persons* sheet. The value must be identical to that in `person:name`.

This field is duplicated for every row of data about the person.

9.2 Person Extra: Unique Identifier

Description

A unique 32 character code assigned to each person in the dataset, as already recorded in the `person:id:admin` field of the *Persons* sheet.

Type of field

Text and numbers

Example of use

a848de4e-eb eb-49d6-9099-7e68ca3b57fc

Spreadsheet column name

`person_extra:id:admin`

Shortcode

`px_id_a`

Sources

No.

Confidence

No.

Guidance on use

This field is used to store the UUID of the person about whom extra information is being entered. The person must already have an entry in the *Persons* sheet. The value must be identical to that in `person:id:admin`.

This field is duplicated for every row of data about the person.

9.3 Person Extra: Gender

Description

Indicators of a person's sex or gender identity, as inferred from pronouns used in the text of available sources.

Type of field

Open list, single choice

Example of use

Male, Female, Other

Spreadsheet column name

person_extra:gender

Shortcode

px_g

Sources

Yes (person_extra:gender:source, px_g_s)

Confidence

Yes (person_extra:gender:confidence, px_g_c)

Guidance on use

This field is used to capture data about the gender of a person, as determined only by the pronouns (“her”, “she”, “his”, “him”, etc) used in any available textual sources about this person. We do not infer a person’s gender from their name or images of them.

Echoing the definition used in the **‘FOAF standard**http://xmlns.com/foaf/spec/#term_gender’, the Person Extra: Gender field is not intended to capture the full range of possible biological, social and sexual associated with the word “gender”. In the majority of cases the value recorded in this field will be *male* or *female*. However, we have left this field open to include alternatives that are expressed within the available sources about a person.

Where the sources contain no textual indication about the person’s gender, the field should be left blank.

9.4 Person Extra: Date of Birth

Description

The date on which a person was born.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

1985-10-01, 1985-10, 1985

Spreadsheet column name

person_extra:date_of_birth

Shortcode

px_dob

Sources

Yes (person_extra:date_of_birth:source, px_dob_s)

Confidence

Yes (person_extra:date_of_birth:confidence, px_dob_c)

Guidance on use

This field is used to capture the date of birth of a person, with as much specificity as allowed by available sources. The field can accept a full or partial date.

9.5 Person Extra: Deceased

Description

Indicates whether a person has died.

Type of field

Positive confirmation, blank if none

Example of use

Y

Spreadsheet column name

person_extra:deceased

Shortcode

px_d

Sources

Yes (person_extra:deceased:source, px_d_s)

Confidence

Yes (person_extra:deceased:confidence, px_d_c)

Guidance on use

Where sources indicate that a person has died, enter Y in the field Person Extra: Deceased. In all other cases, leave the field blank.

In many cases the sources used to evidence Person Extra: Deceased and Person Extra: Date of Death will be the same. In some cases, however, sources may indicate a person has died without specifying a date. In these cases, the field Person Extra: Date of Death should not be filled in.

9.6 Person Extra: Date of Death

Description

A date on which a person died.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2017-07-22, 2017-07, 2017

Spreadsheet column name

person_extra:date_of_death

Shortcode

px_dod

Sources

Yes (person_extra:date_of_death:source, p_dod_s)

Confidence

Yes (person_extra:date_of_death:confidence,p_dod_c)

Guidance on use

Use this field to record the full or partial date of a person's death, as recorded in a source. Where a source reports that a person has died, but does not indicate the date on which this happened, only the field `Person Extra: Deceased` should be filled in.

9.7 Person Extra: Account Type

Description

The name of an online platform or service on which the person holds an account.

Type of field

Text and numbers, chosen from list.

Example of use

facebook, twitter, telegram, whatsapp, youtube, vkontakte, wikipedia

Spreadsheet column name

person_extra:account_type

Shortcode

px_at

Sources

Yes (person_extra:account:source,px_a_s)

Confidence

Yes (person_extra:account:confidence,px_a_c)

Guidance on use

This field is used to record the name of the online platform of service on which a person holds an account. The name is chosen from a list of available platforms and services, which will be updated as required. The subsequent field `Person Extra: Account Identity` is used to record the name of the account held by the person on the platform or service. Sources and confidence fields for `Person Extra: Account Type` are shared with `Person Extra: Account Identity`.

Where a person has more than one account, on the same or different platforms, a new row should be created.

9.8 Person Extra: Account Identity

Description

The account name used by the person on a special online platform or service.

Type of field

Text and numbers

Example of use

tomcopsymes (on Twitter)

Spreadsheet column name

person_extra:account_id

Shortcode

px_aid

Sources

Yes (person_extra:account:source, px_a_s)

Confidence

Yes (person_extra:account:confidence, px_a_c)

Guidance on use

This field is used to record the account name held by the person on a specific online platform or service. The name of the corresponding online platform or service is stored in Person Extra: Account Type.

Sources and confidence fields for Person Extra: Account Identity are shared with Person Extra: Account Name.

Where a person has more than one account, on the same or different platforms, a new row should be created.

9.9 Person Extra: External Link Description

Description

Short textual description of the relevant content of a URL containing information about the person.

Type of field

Text and numbers.

Example of use

Official biography of General Luis Cresencio Sandoval González on the SEDENA website, Wikipedia page for Luis Cresencio Sandoval,

Spreadsheet column name

person_extra:external_link_description

Shortcode

px_eld

Sources

Yes (person_extra:external_link_source, px_eld_s)

Confidence

Yes (person_extra:external_link_confidence, px_eld_c)

Guidance on use

This field is used to store a short description of the content found at an external URL about this person. The details of the external link are stored in the relevant source record. This field is used to gather together resources that provide a high level of detail about the person, and will include official websites, blogs operated by the person, the Wikipedia page about them (if they have one), or Facebook pages credibly linked to the person. Details about the social media footprint of the person are not stored in this field - Person Extra: Account Type and Person Extra: Account Identity are used to capture this data.

The source field associated with `Person Extra: External Link Description` is used to store data about the resource itself, along with other material that evidences why the external link is about the person.

A new row is created for each new resource.

9.10 Person Extra: Media Description

Description

Short textual description of material found in a media resource that provides information about a how person looks or sounds.

Type of field

Text and numbers.

Example of use

“Face and shoulders of Bosco Ntaganda, in military uniform with hat, tie and lapels, backed by two other men in combat fatigues armed with rifles. Taken at a news conference in January 2009.”

Spreadsheet column name

`person_extra:media_desc`

Shortcode

`px_md`

Sources

Yes (`person_extra:media:source, px_m_s`)

Confidence

Yes (`person_extra:media:confidence, px_m_c`)

Guidance on use

This field is used to store a brief description of the content of external. The description should be sufficient for the analyst to quickly appraise what they can expect to find in the media about what the person looks or sounds like. Details about the media type, URL and other metadata are contained in the source associated with `Person Extra: Media Description`.

A new row is created for each distinct media item about the person.

9.11 Person Extra: Notes

Description

Analysis, commentary and notes about the material in row of data in `Persons Extra` that do not fit into the data structure.

Type of field

Text and numbers

Example of use

The image referenced in this row is clipped from a longer video. Should it be necessary, additional views of this individual are available in the video.

Spreadsheet column name

person_extra:notes

Shortcode

px_n

Sources

No.

Confidence

No.

Guidance on use

We use this field to record information about the material recorded in Persons Extra that is likely to provide useful context, additional information that does not fit into the data structure, and notes about how decisions were made about which data to include. Any sources used to write the notes should be included directly inside this field.

10.1 What are incidents?

Incidents are publicly-documented allegations of acts committed by state-controlled security forces that may violate human rights laws and standards, international criminal law and other sets of relevant norms. Incidents may include extrajudicial killings, rape, torture and other forms of violence. Security Force Monitor does not make these allegations itself, but compiles allegations made by governmental bodies, human rights organizations and other civil society actors around the world.

The Security Force Monitor focuses its research on the structure, personnel and operations of security forces; we do not directly investigate specific allegations of human rights abuse in the way that Amnesty International or Human Rights Watch do. As such we consider all reports of human rights abuses as “alleged” in our documentation. This simply means these are claims that other organizations have made and which we are repeating without further verification. The Security Force Monitor does not make allegations against security forces and the data that we publish does not attempt to demonstrate involvement of individuals or units in human rights abuses beyond that which other organizations have alleged.

For each incident, we include data about what happened and when, the location(s) it occurred at, the alleged perpetrators and the type of human rights violation the reporting organization claims has occurred.

In a departure from how we compile data about *Units* and *Persons*, individual fields in incident records are not sourced and rated for confidence. Rather, we provide a single source for the entire incident. This is because each incident is a direct copy of material from a single source rather than a tapestry of material from a range of different sources.

A spreadsheet containing all the fields used by Security Force Monitor can be found in the section called *Sample data entry sheets*.

10.2 Incident: Unique Identifying Number

Description

A unique 32 character code assigned to each incident in the dataset.

Type of field

Text and numbers

Example of use

a407be6a-28e6-4237-b4e9-307f27b1202e

Spreadsheet column name

incident:id:admin

Shortcode

i_id_a

Sources

No

Confidence

No

Guidance for use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs can be created easily using either installable or online tools, for example:

- Linux and OSX users: *uuidgen* command line tool.
- On the web: [UUID Generator](#).

The field is administrative, providing a reliable way to differentiate between different incidents.

When a new incident is created directly in WhoWasInCommand, the platform automatically creates a UUID for that incident and stores it in this field. If a new incident is created in a spreadsheet, the Staff Researcher must generate a unique identifying number for that incident and copy it into the field `incident:id:admin` for the single row associated with that specific incident. This manual, copy-and-paste step is a potential source of error and the Staff Researcher must be careful not to re-use a UUID.

Bulk updates made to WhoWasInCommand.com by spreadsheet import are based on the values in this field. For example, changes made in the row a407be6a-28e6-4237-b4e9-307f27b1202e in the spreadsheet will be applied to the incident with that UUID in WhoWasInCommand.

10.3 Incident: Research Owner

Description

Initials of the Staff Researcher who first created the incident.

Type of field

Text

Example of use

TL, TW, MM

Spreadsheet column name

incident:owner:admin

Shortcode

i_own_a

Sources

No

Confidence

No

Guidance for use

This field is administrative and only used where data are created in a spreadsheet. It is a simple measure to help researchers keep track of records they have created. These data are not imported into WhoWasInCommand. Instead, WhoWasInCommand keeps a record of the changes (edits, new records, deletion) by the name of the system user who made them.

10.4 Incident: Research Status

Description

The place of a row of data in the research workflow.

Type of field

Number range from 0 to 3.

Example of use

1

Spreadsheet column name

`incident:status:admin`

Shortcode

`i_sta_a`

Sources

No

Confidence

No

Guidance for use

This administrative field is only used in spreadsheets. Staff Researchers use this field to indicate where a row of data stands in the research workflow between the first cut of a row of data, review by other researchers, and final readiness for publication. Values in this field are taken from the below controlled list:

- 0: First commit. This row of data has just been added and needs review.
- 1: Fixes needed. A reviewer has made comments that need to be addressed, which will be recorded in the `incident:comment:admin` field.
- 2: Fixes made. The owner of this data has addressed the reviewer's comments.
- 3: Clean. A final check has been made by a reviewer, and this row of data can be published.

Data created and managed in WhoWasInCommand does not use this mechanism. At the time of writing, a simple review system is being implemented in WhoWasInCommand.

10.5 Incident: Research Comments

Description

Observations specific to the process of reviewing data in this row, including fixes, refinements and other suggestions.

Type of field

Text

Example of use

Check location, Missing OSM objects

Spreadsheet column name

incidents:comments:admin

Shortcode

i_com_a

Sources

No

Confidence

No

Guidance for use

This is an administrative field specific to data created in spreadsheets. Staff Researchers use it to pass on feedback about the data in the row. This may include changes needed to specific fields, references to sources that the owner of the row might look at, and other observations that can improve the quality of the data. Data in this field are not intended for publication.

10.6 Incident: Start Date

Description

The date on which an incident started.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

incident:start_date

Shortcode

i_sd

Sources

No

Confidence

No

Guidance for use

If an incident occurred within a single day, Incident: Start Date and Incident: End Date should be the same.

Incidents may occur at some point during a range:

For example: “On or about August 9, 2006, personnel of the NPF paraded 12 alleged armed robbers—including a 12-year-old—before the media at the Central Police Station in Umuahia, capital of Abia State. They claimed to have arrested the suspects after an exchange of gunfire with the police. Some of those in custody had gunshot wounds, and four others were killed during the incident at Olokobe-Ndume community in Umuahia North Local Government Area of Abia State. Following the parade, the police summarily executed the suspects and deposited their bodies at the premises of the Federal Medical Centre in Umuahia. They claimed that the executed victims signed confessional statements before they were killed. On August 17, 2006, the authorities of the Federal Medical Centre arranged a mass burial for the decomposing bodies of the victims. There were no autopsies or inquests. The police later organized a press conference at which they announced the executions.”

We know from this source that the victims were alive as of 9 August 2006 and we know they were dead as of 17 August 2006. However the exact time of the killing occurred is not clear; it could have happened at any point during that time frame. To accommodate this, we would record 2006-08-09 in Incident: Start Date and 2006-08-17 in Incident: End Date.

In keeping with all date fields we include in this dataset, where research indicates that only a year or a year and a month, these partial dates can be included in Incident: Start Date.

10.7 Incident: End Date

Description

The date on which an incident ended.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

incident:end_date

Shortcode

i_ed

Sources

No

Confidence

No

Guidance for use

If Incident: End Date is unclear there are several ways to determine what should be used.

One option is to record the date of interview with victim as Incident: End Date. We can assume that the allegation(s) ended at least the month/day of the interview - or that we at least know they occurred up to that date.

For example: “Abu Bakr, a former detainee in Giwa Barracks told Amnesty International that he had been forced to share a confined area with up to 400 other people [...] Abu Bakr who was held in Giwa barracks told Amnesty International in July 2014: “There was no toilet. To toilet you use a black plastic bag and when you go out you throw it... or if someone used his maybe he will give you.” He also explained: ‘We had rice for breakfast. A small amount, they put it in your hand. You give your hand, they will put the rice, you swallow it, you go back to the cell. Later in the day they give you water once. It is in a jug and you drink and pass it to another inside the cell. In the evening it is rice and stew, small. They give it in a nylon bag. There is no washing, no showers. No sleep. You just sit down only, the place is very tight, just sit on your bottom. You can only pray in the cell where you are sitting.’”

In this example we could record 2014-07 in Incident : End Date because we know that at some time in July he talked to Amnesty International.

Here’s another example:

“Melvin, a 23-year-old sex worker in Port Harcourt, said she was raped twice by the police. She said: “I was arrested twice. Last month they took all of us to Mile 1 police station. We were six that day, we see different people. They put us in different places [in the police station]. We just have to allow them have sex with us. We were detained for three days. We were asked to pay N3,500 each. The one that will bail you will sleep with you. After that you can go.”

In this case, we can look at the footnotes. They often will give the date of when the victim was interviewed. In this case, both footnotes read: “Amnesty International interview in Port Harcourt, October 2011.” - so “last month” would be September 2011 and we would record this as 2011-09 in Incident : Start Date. While they were detained for three days it is unclear if the complete incident occurred in September because Amnesty interviewed this person in October 2011. Accordingly, we could record 2011-10 in Incident : End Date as they could have been arrested on September 29 and then released on 1 October 2011.

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Incident : End Date.

10.8 Incident: Date of Publication

Description

The date of publication of the source used to evidence the incident.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

incident:pub_date

Shortcode

i_pd

Sources

No

Confidence

No

Guidance for use

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Incident: Date of Publication.

10.9 Incident: Date of Last Update

Description

The date of most recent update about the incident.

Type of field

Date (YYYY-MM-DD), fuzzy

Example of use

2012, 2012-11, 2012-11-23

Spreadsheet column name

incident:update_date

Shortcode

i_ud

Sources

No

Confidence

No

Guidance for use

In keeping with all date fields we include in this dataset, where our research can only find a year or a year and a month, this can be included in Incident: Date of Last Update.

10.10 Incident: Status as of Last Update

Description

Most recently available status of the incident.

Type of field

Text, controlled vocabulary

Example of use

Field is not yet implemented.

Spreadsheet column name

incident:update_status

Shortcode

i_us

Sources

No

Confidence

No

Guidance for use

Field is not yet implemented.

10.11 Incident: Location Description

Description

A description of the where the incident occurred.

Type of field

Text and numbers

Example of use

Giwa Barracks, Rikkos neighborhood, Campo Militar Número 6-B

Spreadsheet column name

`incident:location_description`

Shortcode

`i_ld`

Sources

No

Confidence

No

Guidance for use

We use this field to record the location of an incident exactly as described in the source. Here is an example:

“Stanley Adiele Uwakwe and Faka Tamunotonye Kalio were arrested on 10 May and brought to Old GRA detention centre in Port Harcourt. After several days, they were transferred to another police station, but officers there told relatives that the men were not in detention. Unofficially, relatives were informed that the men had been killed by the police.”

While they were detained at “Old GRA detention centre” the location of their killing is unclear. It is also not clear where they were located before they were disappeared - was it at the Old GRA or at the unnamed police station? Since we don’t know we’d leave the `Incident: Location Description` field blank.

Here’s another example of how to use this field:

“And in yet a third case, Human Rights Watch interviewed three witnesses who saw soldiers shoot five men on the Customs Bridge in Maiduguri. One of the victims survived. He told Human Rights Watch that on the afternoon of July 28 soldiers entered a mosque where he was praying with four other men. The soldiers removed their robes, beat them, and marched them to their commander at the bridge. He described what happened next: The soldiers told us to lie down. Four of the soldiers opened fire on us. The commander was watching. I was lying on my side. They saw that some of us were moving and shot us again. I then lost consciousness. I regained consciousness in the night and dragged myself to an area in the dirt near Dandal Community Bank. I spent the night under a bus. In the morning an achaba [commercial motorcycle taxi] man who knew me took me to my house. My family called a doctor... They removed four bullets from my body. A former Boko Haram member who witnessed the shootings

at the Customs Bridge insisted to Human Rights Watch that the five men were not Boko Haram members. According to him, “The old man was holding prayer beads, and Boko Haram members don’t do that. The two youth wore T-shirts and the [other] two men wore long pants, not the short pants of Boko Haram.” The soldiers left the corpses on the bridge for three days.”

The location we would enter into Incident: Location Description would be “the Customs Bridge”, while we would enter Maiduguri into the field called Incident: Site, Settlement (a field that is documented below).

A common issue is the separation of specific incidents contained within a single account of violations based on geography.

Often a person is arrested and, for example, beaten at a specific site (and the account might include information about other victims being killed at the site of arrest). They are then transported to another site where they are detained and tortured. Moreover, the conditions during the transportation of detainees/prisoners may amount to violations of fundamental rights and often the narrator describes people dying while being transported.

In such instances, researchers should consider the initial arrest and transportation to the site of detention to be one incident and abuses committed or otherwise tied to site of detention a separate incident.

10.12 Incident: Location

Description

Type of field

Text and numbers; linked to `location:humane_id_admin`.

Example of use

Baga (osm, point) 4d7d97a6-d85e-436b-9511-81e8d55ceff3

Spreadsheet column name

`incident:location`

Shortcode

`i_loc`

Sources

No

Confidence

No

Guidance on use

This field is used to store information about the Location where an incident happened. The value included in this field must be taken from `location:humane_id:admin` in the *Locations* dataset. For further guidance on the creation, management and use of Locations visit the *Locations* documentation.

10.13 Incident: Violation type

Description

Type of alleged violation of human rights law, international humanitarian law or other relevant laws committed during the incident.

Type of field

Text, multiple entry, controlled vocabulary

Example of use

Torture; Violations of the Right to Life, Intentionally directing attacks
against the civilian population

Spreadsheet column name

incident:violation_type

Shortcode

i_vt

Sources

No

Confidence

No

Guidance for use

In Incident: Violation Type, a values is taken “as is” from the source. If the source states “torture”, we transcribe this without further analysis.

This field can accept multiple entries. If the field is created in a spreadsheet, the discrete entries must be separated with semi-colon.

10.14 Incident: Violation Description

Description

A description of the incident.

Type of field

Text and numbers

Example of use

According to Amnesty International: “Usman Modu, a 26-year-old scrap metal dealer from Maiduguri, spent almost two and a half years in Giwa barracks. He was arrested in April 2012 in Gwange, Maiduguri, during a screening operation after a Boko Haram attack. All the people who left the mosque were gathered together: the elderly and children were allowed to go home. The men were brought before a “pointer”, who pointed at him and 17 other men. He was first taken to a JTF station called NEPA and then to Giwa Barracks. “One by one we were brought in front of an armoured tank. I never saw anything. People said there was someone inside. When I went up, soldiers said I should go left. They started beating me. One soldier beat me with his gun and I fell down. They tied my hands behind my back and beat me. Then told me to go inside the car. I don’t know why I was chosen. I was surprised, I don’t know what I have done.” The military released Usman with 41 others in November 2014. The 17 men arrested with Usman all died in military custody.”

Spreadsheet column name

incident:violation_description

Shortcode

i_vd

Sources

No

Confidence

No

Guidance for use

In this field we record a direct quotation from the civil society, governmental or other source that describes the incident. When an incident has more than one report tied to it, start the quotation as below:

According to X organization, "Description of incident". According to Y organization, "Description of incident".

10.15 Incident: Perpetrator Person Unique Identifier

Description

The UUID of the person named in Incident: Perpetrator Person Name.

Type of field

Text and numbers; linked to `person:id:admin`.

Example of use

251be336-e67b-4e44-bc0d-97d4e8188b44

Spreadsheet column name

`incident:perpetrator_person_id:admin`

Shortcode

`i_ppid_a`

Sources

No

Confidence

No

Guidance on use

This value in this field should be the same as the value in `persons:id:admin` of the person named in Incident: Perpetrator Person Name.

10.16 Incident: Perpetrator Person Name

Description

The name of the person alleged to have committed the act(s) described in the incident.

Type of field

Text and numbers, multiple entry; linked to `person:name`.

Example of use

Friday Iyamabo

Spreadsheet column name

incident:perpetrator_person_name

Shortcode

i_ppn

Sources

No

Confidence

No

Guidance for use

If a person or persons are named in the sources for the incident, we will record this information in the Incident : Perpetrator Persons Name field. The value in Incident : Perpetrator Person Name will correspond to a value in Person : Name.

For example: “Nwanneka narrated to NOPRIN researchers her experience at the SCID in Enugu in May 2002. She was initially arrested with two other females by officers of the Ninth Mile Police Station on the outskirts of Enugu on charges of assisting an armed robbery suspect, before being transferred to the SCID on May 3, 2002. After taking the statements of the female detainees, NPF Inspector Friday Iyamabo ordered them detained in the cells of the SCID. He later reportedly returned to the cell with pepper spray and powdered chili pepper, ordered the female detainees to strip and one after the other applied the mixture of pepper spray and chili to their genitals after severely beating them with batons. The detainees were denied access to medical treatment. Five years after this experience, Nwanneka reported to NOPRIN researchers in April 2007 that, as a result of this experience, she continues to suffer from complications with both her reproductive system and urinary tract.”

In this case, the alleged perpetrator is named in the source report. We would record the name Friday Iyamabo in the field Incident : Perpetrator Person Name.

10.17 Incident: Perpetrator Unit Unique Identifier

Description

The UUID of the unit named in Incident : Perpetrator Unit Name.

Type of field

Text and numbers; linked to unit:id:admin.

Example of use

a27d4e1f-7add-4302-ab2e-70c426cce519

Spreadsheet column name

incident:perpetrator_unit_id:admin

Shortcode

i_puid_a

Sources

No

Confidence

No

Guidance on use

This value in this field should be the same as the value in `unit:id:admin` of the unit named in `Incident:Perpetrator Unit Name`.

10.18 Incident: Perpetrator Unit Name

Description

The unit(s) alleged to have committed the act(s) described in the incident.

Type of field

Text and numbers, multiple entry; linked to `unit:name`.

Example of use

2 Batallón de Fuerzas Especiales

Spreadsheet column name

`incident:perpetrator_unit_name`

Shortcode

`i_pun`

Sources

No

Confidence

No

Guidance for use

If the source for the incident states that specific units committed the alleged human rights violations described in the incident, we include these names in `Incident: Perpetrator Unit Name`. The value in `Incident: Perpetrator Unit Name` will correspond to a value in `Unit: Name`.

Here is an example of source material that contains information that would be included in `Incident: Perpetrator Unit Name`:

According to the United States Department of State, Bureau of Democracy, Human Rights and Labor: “On March 24, the JTF reportedly killed four men near Isaka in the Okrika Local Government Area, Rivers State, when they confronted them and other armed men attempting to hijack a barge. There was no investigation conducted.”

In this case, we would search `Unit: Name` for the canonical entry for “JTF” and include it in the field `Incident: Perpetrator Unit Name`.

10.19 Incident: Perpetrator classification

Description

General branch or tier of the security force alleged to have committed the act(s) described in the incident.

Type of field

Text and numbers, multiple entry, controlled vocabulary taken from Unit: Classification

Example of use

Army, Ejército, Police, Military, Military Police ; Joint Operation

Spreadsheet column name

incident:perpetrator_classification

Shortcode

i_pcl

Sources

No

Confidence

No

Guidance for use

Sometimes a source will report general information about the alleged perpetrators of an act. For example, rather than state a unit or a specific person the source might include something generic like “soldiers” or “police”. In cases like these where we can’t be more specific we use this field to record the branch or general classification of the force implicated in the incident. For example:

According to Amnesty International: “On 1 May 2012, around midnight, Nigerian soldiers arrested 37-year-old Dungus Ladan (not his real name), at his home in Maiduguri. Fatima, Dungus’ wife, told Amnesty International that the soldiers promised to just take him for an interrogation that should not last more than a few hours. When her husband did not return, she said, his father went on 3 May to Giwa barracks to check what had happened. Soldiers told him that Dungus had already been released. When he still did not return, the father went back again to the barracks, where soldiers told him that he should come back the next day to bail out his son. The following day, several relatives went together and gave the soldiers “what they could,” and the soldiers again promised to release Dungus that day. His wife said that the soldiers kept asking for money, and the family kept paying, but Dungus was never released. In February 2014, his father saw Dungus in the detention facility; they spoke briefly. Dungus said he had been framed by some people who owed him money and they arranged for him to be arrested and detained. Since then, his family has not seen him again; soldiers at Giwa barracks have told them he is not there.”

The only alleged perpetrators described in this alleged incident are “soldiers”. The most appropriate term to enter in Incident: Perpetrator Classification to match this description which would be “military” because “soldiers” could refer to personnel of the Army, Navy or other armed services of a country.

Entries in Incident: Perpetrator Classification correspond to those in Unit: Classification.

10.20 Incident: Source

Description

The UUID of the access point in the source that provides information about the incident.

Type of field

Text and numbers, chosen from list

Example of use

5b8362d6-b13a-4764-9ff0-2d7cfd7d5f37

Spreadsheet column name`incident:all:source`**Shortcode**`i_all_s`**Sources**

No

Confidence

No

Guidance for use

Unlike data captured about `units` or `person`, data about `incidents` are not sourced at the level of each individual field. Instead, we have a single source for the whole incident. The entry in `Incident: Source` should be a Unique Identifier (“UUID”) for a source access point that has been already created in the master list of sources. The relevant values will be found in the field `Source: Access Point Unique Identifier`.

11.1 What are Locations?

Locations are unique places or positions. A named town or city can be a Location, as can an administrative area like a county, district or state. In fact, anything that be drawn on a map can be a Location: a specific point, a section of a road, a military line of control, and so on.

In the Security Force Monitor (SFM) data model, Locations are a primary entity; this means we manage them as a discrete set of datapoints that can be referenced in other parts of the dataset. Locations are the way we describe the “sites” and “areas of operation” of *Units*. Locations describe the geographic footprint of security forces, including their infrastructure (bases, facilities, checkpoints, air fields, bunkers), as well as their territorial jurisdictions and operations as they change over time. We also use Locations to describe the places where security force units are alleged to have committed human rights abuses.

To define a Location, we start with information included in the sources that underpin all our research (see *Data integrity measures* and *Sources*). The Location descriptions contained in sources vary greatly in their precision and accuracy:

- At a precise coordinate: “Artillery Brigade deployed to latitude x, longitude y”.
- At a very specific place: “Has a checkpoint on the corner of street A and street B in Test Town”.
- At a very specific named place: “Based at Famous General Army Camp in Test Town”.
- At a nonspecific place in a particular settlement: “In Test Town”.
- In a named subdivision of a particular settlement: “Suburb A in Test Town”.
- In a named but nonspecific place near a particular settlement: “At the Smoth family borehole north of Test Town”
- In a nonspecific place near a particular settlement: “Around Test Town”.
- In a definable area that is not a settlement: “In Test County”.
- In an area that is difficult to define: “Somewhere in the north of the country”

When we have decided on what Location is actually described in the source, we use the fields in this standard format to capture and structure data about the Location. We can do this by consulting existing sources of geospatial information

like [OpenStreetMap](#), [Humanitarian Data Exchange](#), commercial mapping services like Google Maps, and (where they exist) data provided by the relevant national geospatial agencies. We reconcile the information we gain from the sources with options provided to us by a number of geospatial information sources, which we then turn into a Location.

For example, if a source describes a place called “Potiskum” in Yobe State, Nigeria we can [look it up on OpenStreetMap](#). From this record, we can capture the Location’s name, object ID number (255322295) and its geometry type (a “node”, which is a “point” for our purposes). We enter this basic data about the Location into the Location fieldset, generate a UUID for it (41b3aec7-d88e-4ef1-a7d8-1b7fdf81a20c), and create a “human readable” key that we can then use to reference this specific Location in other parts of the data model (Potiskum (osm, point) 41b3aec7-d88e-4ef1-a7d8-1b7fdf81a20c). We can then use SFM’s `geo` automation tool to obtain more information from OpenStreetMap about this Location, including its geometry (in this case, a co-ordinate pair), additional metadata (such as a name in Arabic or other local languages), and the various administrative areas (like states, local government areas, wards) in which it is sited. This additional information enables us to plot the Location on a map, and opens up a whole range of opportunities for geospatial analysis.

Where there is not a good option in an existing geospatial data source, and where the source contains sufficient descriptive information, we can create the Location data directly using a Geographical Information System (GIS) tool like QGIS, Earth Pro or Google My Maps. This method is useful for describing Locations that may emerge from geolocation processes, such as views portrayed in images and other subjective descriptions of a place.

We create a datasets of Locations for each country we work on. These data are stored in a spreadsheet (or delimited text file like `.csv` or `.tsv`) and a corresponding GeoJSON file that contains everything in the spreadsheet as well as every Location’s geometry and any additional metadata about the Location provided by the geospatial information source. The two files provide views of the data that are useful for different purposes. The `.tsv` can be easily updated using a spreadsheet, but it’s not the right place to store the geometry; the GeoJSON is more useful to developers and can be pulled in a geographica information system (GIS) for analysis and visualisation. We keep the two files synchronised. Storing the Location data this way also means we retain a standalone copy in robust and easily-processed formats of all the data we need.

The Location model described in this documentation replaces an earlier approach that stored the full metadata about a Location alongside the data on Units and Incidents. Maintaining the Location information using the earlier approach involved a great deal of duplication and introduced more opportunities for error. This updated approach brings the management of Location information into a single place and idiom, enables more effective use of automation tools, and extends the range of data we can capture and manage about Locations.

11.2 Location: Research Status

Description

The place of a row of Location data in the research workflow.

Type of field

Text and numbers; controlled vocabulary.

Example of use

3, X

Spreadsheet column name

location:status:admin

Shortcode

l_sta_a

Sources

No

Confidence

No

Guidance on use

Staff Researchers use this field to indicate where a row of data stands in the research workflow between the first cut of a row of data, review by other researchers, and final readiness for publication. Values in this field are taken from the below controlled list:

- *X*: Row should be deleted.
- *0*: First commit. This row of data has just been added and needs review.
- *1*: Fixes needed. A reviewer has made comments that need to be addressed, which will be recorded in the `Locations:comments:admin` field.
- *2*: Fixes made. The owner of this data has addressed the reviewer's comments.
- *3*: Clean. A final check has been made by a reviewer, and this row of data can be published.

This field is common to all main entities in the SFM data model.

11.3 Location: Research Comments

Description

Observations specific to the process of reviewing data in this row, including fixes, refinements and other suggestions.

Type of field

Text

Example of use

Location does not exist in OpenStreetMap - alternate gazeteer needed, Possible duplicate of Location 1bbdfd2b-2d7c-4677-8elf-8fa5b0367cfe, Reprocess to update geometry

Spreadsheet column name

`location:comments:admin`

Shortcode

`l_com_a`

Sources

No

Confidence

No

Guidance on use

Staff Researchers use this administrative field to pass on feedback about the data in the row. This may included changes needed to specific fields in that row, references to sources that the owner of the row might look at, and other observations that can improve the quality of the data. Data in this field are not intended for publication. The workflow of Location datapoints is a little different from other entities within the SFM data model, in that it is a combination of manual work by Staff Researchers and automation work by developers. The comments field is commonly used to flag places where developers may need to provide assistance. The comments field is common to all main entities in the SFM data model.

11.4 Location: Unique Identifier

Description

A unique 36-character code assigned to each Location in the dataset.

Type of field

Text and numbers

Example of use

5f55f3f1-ed83-4766-b26a-fd11bedc398c

Spreadsheet column name

location:id:admin

Shortcode

l_id_a

Sources

No

Confidence

No

Guidance on use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs must be created using either installable or online tools, for example:

- Linux and OSX/MacOS users: *uuidgen* command line tool.
- On the web: [UUID Generator](#).

The field is administrative, providing a reliable way to differentiate between different Locations. ID fields are common to all main entities in the SFM data model.

When a new Location is created in a spreadsheet, the Staff Researcher must generate a unique identifying number for the Locations and copy it into the field `location:id:admin`. This manual, copy-and-paste step is a potential source of error and the Staff Researcher must be careful not to re-use a UUID.

Bulk updates made to WhoWasInCommand.com by spreadsheet import are based on the values in this field. For example, changes made in the row `a407be6a-28e6-4237-b4e9-307f27b120e` in the spreadsheet will be applied to the Location with that UUID in WhoWasInCommand.

11.5 Location: Human-Readable Unique Identifier

Description

A human-readable unique identifier for each Location in the dataset.

Type of field

Text and numbers

Example of use

Ta'izz Governorate (osm, poly) 5c35b342-0b5e-4648-86cd-7ad730d647fa

Spreadsheet column name


```
location:humane_id:admin
```

Shortcode

```
l_hid_a
```

Sources

No

Confidence

No

Guidance on use

The values in `location:humane_id:admin` are a concatenation of four other values in the row of data. They provide a unique but human-readable key that can be included in Units and Incidents data to refer to a specific Location within the `Locations` dataset. The field is created by following the below format:

```
location:name (Location:origin, Location:geotype) Location:id:admin
```

The value `Ta'izz Governorate (osm, poly) 5c35b342-0b5e-4648-86cd-7ad730d647fa` tells us that the name of the place is Ta'izz Governorate, that it is a Location found in `osm` (short for “Open-StreetMap”) that it denotes an area (`poly`); the UUID provides the hard link to a specific row in the Location table.

Values in `location:humane_id:admin` are used by Staff Researchers to reference a Location in other data tables. For example, when defining a site or area of operations in the *Units* tables, a value from `location:humane_id:admin` is used. The reason for this particular formulation is the need to balance readability with uniqueness. We could choose to use the UUID in `location:id:admin` as a way to reference Locations in other tables, but this would not give any indication about where the Location was, or what sort of Location it was. Similarly, the values in `location:name` could be used as a reference to a Location, but these are not unique enough for us to be certain that we are referencing the correction Location. The format we have chosen balances these competing needs, giving the user a quick way to see the name of a Location, what type of object it is, where we got it from, along with its UUID.

11.6 Location: Object Name

Description

The name of the Location as specified in the source of geospatial information from which it is taken.

Type of field

Text and numbers

Example of use

```
`Ta'izz Governorate`
```

Spreadsheet column name

```
location:name
```

Shortcode

```
l_n
```

Sources

No

Confidence

No

Guidance on use

Locations are a combination of metadata entered by hand and other data obtained through use of automation tools. Locations are also derived from different data sources that may describe geographic objects in a variety of ways. The value in `location:name` is to be taken directly from the geospatial data source. For example, if a Location is derived from OpenStreetMap, we take the value from OSM's `name` field and place it in `location:name`. Along with `location:id` and `location:geo_type`, `location:name` is needed in order for automation tools to identify the object within the geospatial data source. Where a Location is arbitrarily-defined, or is derived from a data source that does not provide a name, the Staff Researcher can provide one.

11.7 Location: Object Identifier

Description

The identifier for the Location as specified in the source of geospatial information from which it is taken.

Type of field

Text and numbers

Example of use

383895

Spreadsheet column name

`location:id`

Shortcode

`l_oid`

Sources

No

Confidence

No

Guidance on use

Locations are a combination of metadata entered by hand and other data obtained through use of automation. Locations are also derived from different data sources that may describe geographic objects in a variety of ways. The value in `location:id` is to be taken directly from the geospatial data source. For example, if a Location is derived from OpenStreetMap, we take the value from OSM's `id` field and place it in `location:id`. Along with `location:name` and `location:geo_type`, `location:id` is needed in order for automation tools to identify the object within the geospatial data source. Where a Location is arbitrarily defined, or is derived from a data source that does not provide a ID number, the Staff Researcher can provide one.

11.8 Location: Object Geometry Type

Description

The two-dimensional geometric primitive of the Location, as defined in the source of geospatial information from which it is taken.

Type of field

Text

Example of use

point, poly

Spreadsheet column name

location:geo_type

Shortcode

l_gt

Sources

No

Confidence

No

Guidance on use

This field used a controlled vocabulary to describe the type of geometry used to represent the Location on a map. The Staff Researcher can choose from the following three options?

- **point**: the Location is a single distinct point on a map, represented by a single pair of geographic coordinates.
- **poly**: the Location is a closed area on a map, its boundary described by a sequence of geographic coordinates.
- **line**: the Location is a line on a map, described by a sequence of geographic coordinates. A line may also be closed.

The gazetteer used as the source of geometry may used different terminology to describe the Location. For example, in OpenStreetMap the boundaries of administrative areas (such as counties or states) *are described* using an object called a *relation*; although this can be a complex mix of different objects, for our purposes it is a *poly* because it describes an area.

Along with the values in `location:name`, `location:id` and `location:id:admin` the value entered in `location:geo_type` becomes part of the Location's "humane id", a human-readable unique identifier that acts as a reference for a Location when it is used in other parts of the data model (such as when defining a "site" in the *Units* data, for example).

11.9 Location: Origin

Description

The geospatial information source that provides information about this Location.

Type of field

Text and numbers

Example of use

osm, sfm, hdx

Spreadsheet column name

location:origin

Shortcode

l_o

Sources

No

Confidence

No

Guidance on use

SFM uses a combination of manual data entry and automated processes to manage Location information. The values in `location:origin` identify where automation tools should go to obtain spatial information about an object. For example, if the value `osm` is entered in `location:origin` this indicates that the automation tool should query OpenStreetMap in order to obtain spatial information about a Location. If `osm` were set, then the values in `location:name` and `location:id` would correspond to the object name and ID number in OpenStreetMap. Locations can be derived from comprehensive online services, as well as other sources like locally-held `.shp` or `.kml` files. The number of origins is unlimited.

11.10 Location: Source

Description

The UUID of the access point in the source that provides information about the Location.

Type of field

Text and numbers

Example of use

20248d51-6efe-4150-a5b6-4211fd83365d

Spreadsheet column name`location:source`**Shortcode**`l_s`**Sources**

No

Confidence

No

Guidance on use

SFM uses a number of different sources of geographical information, including OpenStreetMap, data provided by the United Nations through the Humanitarian Data Exchange, and Locations that are arbitrarily defined during research. Staff Researchers should use the `location:source` field to make note of exactly which dataset has been used as a source of this Location. The UUID will reference an entry in the [Sources](#) dataset. In this way, the `location:source` field serves a different purpose to `location:origin`.

11.11 Location: Country

Description

Country in which the Location is situated.

Type of field

Text, controlled vocabulary

Example of use

ye, ng, mm

Spreadsheet column name

location:country

Shortcode

l_c

Sources

No

Confidence

No

Guidance on use

Values for this field are the ISO 3166-1 alpha-2 country codes, which can be found ([on the ISO website](#) and on [Wikipedia](#)). This field is entered manually by the Staff Researcher and acts as a simple cross-check on the automatically-populated values in location:admin_level_2.

11.12 Location: Admin Level

Description

The administrative level of the Location described in the row, if defined in the source of geographical information from which the Location is derived.

Type of field

Numbers; programatically created.

Example of use

2

Spreadsheet column name

location:admin_level

Shortcode

l_al

Sources

No

Confidence

No

Guidance on use

In every country, places are organized hierarchically based on their political significance, population and other factors. This feature passes into geographical information systems. At the top of the hierarchy rests the international boundary and capital city of a country; beneath this, there are sub-national divisions like states or provinces, and regional

capitals, followed by districts, counties, municipalities, towns, suburbs, wards and so on. Different countries have different ways of describing these political and administrative divisions, but they are largely hierarchical and can be cross-compared. Knowing the level(s) at which a Location sits in the overall hierarchy provides us with a useful way to group and understand Locations; it can tell us important things about political and administrative authority, governance and elections, as well as security force jurisdictions and organizational structures.

The field `location:admin_level` is drawn from OpenStreetMap, which has a [comprehensive table](#) that matches the divisions that exist in every state to a single ranking scheme from 2 (international border) to 10 (small villages and communities). Some countries have defined a level 11 division, but we do not use this. Not all levels are present in every country: for example, Mexico does not define a level 3 administrative area.

The data in `location:admin_level` and the other “admin_level” fields are automatically populated using a script that queries the OSM Overpass API. The Staff Researcher does not do this manually.

11.13 Location: Admin Level 10

Description

The administrative level 10 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically created.

Example of use

San Roque (osm, poly) 78dd704f-12ba-4b38-b887-41efd0d803fb, a *barangay* located in the [Philippines](#).

Spreadsheet column name

`location:admin_level_10`

Shortcode

`l_al10`

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the level 10 administrative area in which the current Location is situated. Level 10 is a extremely small administrative division, and is rarely specified in freely available geospatial information sources.

The [schema used by OpenStreetMap](#), for example, includes *quartiers* (Belgium), *asumid* (subdistricts of Tallinn, Estonia) and (neighbourhoods of Damascus, Syria) in the list of types of level 10 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.14 Location: Admin Level 9

Description

The administrative level 9 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Zone 13 (osm, poly) b858ac31-9e46-4818-b70a-572756d60012, a *barangay zone* in the Philippines.

Spreadsheet column name

location:admin_level_9

Shortcode

l_al9

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (location:humane_id:admin) of the level 9 administrative area in which the current Location is situated. Level 9 is a extremely small administrative division, and is rarely specified in freely available geospatial information sources.

The [schema used by OpenStreetMap](#), for example, includes *arangay zones* (Philippines), *Sectores y Barrios de 1° nivel* (Venezuela) and (townships in Myanmar) in the list of types of level 9 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.15 Location: Admin Level 8

Description

The administrative level 8 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Ermita (osm, poly) 9989ba43-3b03-473a-8226-511a8eb82c3d, an *administrative district* of Manila in the Philippines.

Spreadsheet column name

location:admin_level_8

Shortcode

l_al8

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the level 8 administrative area in which the current Location is situated. Level 9 is a relatively small administrative division, and may not be commonly found in freely available geospatial information sources.

The [schema used by OpenStreetMap](#), for example, includes *city corporations* (Bangladesh), *cantons* (Chad) and *kebele* (Ethiopia) in the list of types of level 8 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.16 Location: Admin Level 7

Description

The administrative level 7 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Wuse II (osm, poly) 111f698a-421e-4fc8-9ace-c0aa62b461b5

Spreadsheet column name

`location:admin_level_7`

Shortcode

`l_al7`

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the level 7 administrative area in which the current Location is situated. Level 7 areas are commonly found in freely available geospatial information sources such as OpenStreetMap.

The [schema used by OpenStreetMap](#), for example, includes *sous-préfectures* (Chad), *arrondissements* (in the cities of Ouagadougou and Bobo Dioulasso, Burkina Faso) and *microrregiões* (micro-regions in Brazil) in the list of types of level 7 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.17 Location: Admin Level 6

Description

The administrative level 6 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Arbinda (osm, poly) 659c231e-eb1e-4c46-a710-b7663ef9f2e0, a *commune rurale* in Burkina Faso.

Spreadsheet column name

location:admin_level_6

Shortcode

l_al6

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (location:humane_id:admin) of the level 6 administrative area in which the current Location is situated. Level 6 areas are commonly found in freely available geospatial information sources such as OpenStreetMap.

The [schema used by OpenStreetMap](#), for example, includes *départments* (Chad), *municipios* (Mexico) and local government areas (Nigeria) in the list of types of level 6 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.18 Location: Admin Level 5

Description

The administrative level 5 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Seti (osm, poly) 64a4dd09-36d4-4455-bd07-a77addc91946, a *zone* in Nepal.

Spreadsheet column name

location:admin_level_5

Shortcode

l_al5

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the level 5 administrative area in which the current Location is situated. Level 5 areas are commonly found in freely available geospatial information sources such as OpenStreetMap.

The [schema used by OpenStreetMap](#), for example, includes the *préfecture* (Togo), *Provincial legislative districts* (Philippines) and *regions* (Côte d'Ivoire) in the list of types of level 5 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.19 Location: Admin Level 4

Description

The administrative level 4 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programmatically generated.

Example of use

Gombe (`osm, poly`) 06791bb5-c39d-4a32-a05b-f3945c4f83ea, a [state in Nigeria](#).

Spreadsheet column name

`location:admin_level_4`

Shortcode

`l_al4`

Sources

No

Confidence

Text and numbers; programmatically generated.

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the level 4 administrative area in which the current Location is situated. Level 4 areas are commonly found in freely available geospatial information sources such as OpenStreetMap, and are usually the largest sub-national administrative areas.

The [schema used by OpenStreetMap](#), for example, includes provinces (Philippines), states (Nigeria) and *régions* (Mali) in the list of types of level 4 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.20 Location: Admin Level 3

Description

The administrative level 3 Location within which the present Location is wholly situated.

Type of field

Text and numbers; programmatically generated.

Example of use

Central Visayas (osm, poly) 81848978-3998-48bf-87a7-bd1888912aee, a [region of the Philippines](#).

Spreadsheet column name

location:admin_level_3

Shortcode

l_al3

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (location:humane_id:admin) of the level 3 administrative area in which the current Location is situated. Where defined, level 3 administrative areas are commonly found in freely available geospatial information sources such as OpenStreetMap.

The [schema used by OpenStreetMap](#), for example, includes regions (Philippines) in the list of types of level 3 administrative area.

This field is programmatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.21 Location: Admin Level 2

Description

The administrative level 2 Location - the international state boundary - within which the present Location is wholly situated.

Type of field

Text and numbers; programatically generated.

Example of use

Mali (osm, poly) 8e7b492e-5346-4f43-91a0-55c1f3419468, Sudan (osm, poly) 7117df90-1e52-4726-806a-8e422a0511c6

Spreadsheet column name

location:admin_level_2

Shortcode

l_al2

Sources

No

Confidence

No

Guidance on use

This field contains the human-readable identifier (`location:humane_id:admin`) of the international boundary of a state, also known within the OpenStreetMap schema of administrative areas as a level 2 boundary. This field is programatically generated using a geospatial query; the Staff Researcher does not enter this manually.

11.22 Location: Notes

Description

Analysis, commentary and notes about the Location that do not fit into the data structure.

Type of field

Text and numbers

Example of use

Sources show Location is within the forested areas between two villages and is derived through geolocation and image analysis of source eeb13cf1-7b98-4075-a09b-530146d2ee37

Spreadsheet column name

`location:notes:admin`

Shortcode

`l_n_a`

Sources

No

Confidence

Yes

Guidance on use

We use this field to record information about the Location that is likely to provide useful context, additional information that does not fit into the data structure, and notes about how decisions were made about which data to include. Any sources used should be referenced directly inside the field. Notes are intended to be published.

11.23 Location: First Check Time

Description

Timestamp of the first time that metadata and geometry for this Location was obtained programatically from OpenStreetMap Overpass API.

Type of field

Datetime; programatically generated.

Example of use

`2021-02-14T19:39:01Z`

Spreadsheet column name

`location:first_check_time`

Shortcode

`l_fct`

Sources

No

Confidence

No

Guidance on use

After Staff Researchers have entered the minimum metadata for a Location, we use a script to obtain further information about that object from OpenStreetMap's Overpass API. Overpass gives us the full set of metadata tags for the Location (such as its name in local languages, its last date of update and so on) as well as the geometry that we use to plot the Location on a map. As Location objects can change over time, we keep a record of the date and time at which we first obtained the extended metadata from OSM, as well as the most recent.

This is a programmatically generated field; the Staff Researcher should not enter this directly.

11.24 Location: Last Check Time

Description

Timestamp of the most recent time that metadata and geometry for this Location was obtained programmatically from OpenStreetMap Overpass API.

Type of field

Datetime; programmatically generated.

Example of use

`2021-02-15T20:33:02Z`

Spreadsheet column name

`location:last_check_time`

Shortcode

`l_lct`

Sources

No

Confidence

No

Guidance on use

After Staff Researchers have entered the minimum metadata for a Location, we use a script to obtain further information about that object from OpenStreetMap's Overpass API. Overpass gives us the full set of metadata tags for the Location (such as its name in local languages, its last date of update and so on) as well as the geometry that we use to plot the Location on a map. As Location objects can change over time, we keep a record of the date and time at which we first obtained the extended metadata from OSM, as well as the most recent.

This is a programmatically generated field; the Staff Researcher should not enter this directly.

11.25 Location: Error

Description

Errors encountered during automated processing of a Location.

Type of field

Text and numbers; programatically generated.

Example of use

not found, Name changed to 'Arbindah'

Spreadsheet column name

location:error

Shortcode

l_err

Sources

No

Confidence

No

Guidance on use

SFM's `geo` tool will use this field to describe any problems it has in obtaining extended metadata about geometry of a Location from OpenStreetMap Overpass API. It populates this field each time the script it run; developers should use the messages to fix the underlying problem with the Location, after which `geo` can be re-run. The field is programmatically generated, and the Staff Researcher should not manually enter anything in this field.

11.26 Location: “As of” Date

Description

The date and time of the old version of an OpenStreetMap item that we want to retrieve.

Type of field

Datetime

Example of use

2009-03-24T07:50:06Z

Spreadsheet column name

location:as_of_date

Shortcode

l_aod

Sources

No

Confidence

No

Guidance on use

OpenStreetMap is created by its users and every update to any object on the map is recorded and stored. This means you can see the history of an object, and that changes to the map can be observed, discussed and reverted if necessary. The version history of a map object is also important for SFM research, because it may give us a way to access earlier representations of administrative geography. Borders and boundaries change all the time, and these changes are often reflected in the map's history. It also means that we can protect the integrity of our own data by indicating that the Location is based on an OpenStreetMap object *as it was* at a particular date and time.

The feature of OpenStreetMap that enables this is the repository of [attic data](#), and it can be queried using the Overpass API (directly or by using the SFM `geo` tool). The value the Staff Researcher enters into `location:as_of_date` must correspond a value listed in the version history of an object. This information is accessible by selecting “View history” on any OSM object, followed by “Download XML”. Here is [an example of the attic data for Ermita](#), a level 9 administrative area in then Philippines.

12.1 What are sources?

Security Force Monitor collects data about the persons and units that comprise security forces, along with allegations of human rights abuses made against security forces. This data is carefully collected from a variety of sources, generally online. These include:

- Laws of the country;
- Official government media;
- Press releases from the relevant ministries of the country (Information, Defense, Interior, and others);
- Security force newsletters;
- Social media pages for security services or government agencies;
- Other social media and messaging services;
- Statistics and data agencies;
- Local government websites;
- Human rights commissions;
- Third country government publications and other documents;
- United Nations publications and other documents;
- Local news reportage;
- Civil society and human rights reporting;
- Academic research; and,
- Other country-specific sources.

We also identify non-digital resources such as monographs, scholarly literature, biographies and other materials about security services. The existence and availability of these type of sources vary widely from country to country.

Sources can also be published in a range of different media forms, not only text. Other media forms may include maps, images, audio recordings, video, social media posts, messages sent through messaging services. We have designed the data capture format for sources to be flexible enough to accommodate a wide range of different media.

A spreadsheet containing all the fields used by Security Force Monitor can be found in the section called *Sample data entry sheets*.

12.2 Sources and Access Points

When we choose to use a source as evidence for a data point, we create a spreadsheet or database entry for it. This entry includes the data required to identify the source: title, publication date, URL, name of publication and so on.

However, a source can have multiple “access points”. An access point directs us to a particular part of a source as evidence for a data point - it’s much like a citation in an academic paper. This could be material from a specific page in the source; it could also be a specific archive snapshot of a page, as the content of a webpage can sometimes change over time even though its basic identifying data will not. In this way, a single source can have multiple access points.

There are seven ways that an access point can be “carved out” of a specific source, taking in account the source’s media type:

- **archive**: an archive snapshot of the source contains different content from the source, or from other snapshots.
- **page**: a page or range of page in a document source like a book or report.
- **line**: a line or range of lines in a line-numbered document like an interview transcript.
- **clip**: a passage from a video or audio source, comprising a start time and a stop time.
- **frame**: a single capture point from a video.
- **still**: an image captured from a video or interactive resource which does not correspond to a specific frame.
- **paragraph**: where a document is numbered throughout, such as in United Nations Security Council documents, paragraphs can be used as access point triggers.

Here are some examples of how access points based on archives and pages work in practice:

- *Access points based on differences between archive snapshots*: The website of the Bangladesh Police used to publish a page describing the subordinate units of “Dhaka Range”. Although this page is no longer live it has been captured in the Internet Archive at various points in time between 2013 and 2018. An assessment of the snapshots shows that though the title, publisher and URL don’t change, there are important differences in the content of the webpage. A 2013 snapshot contains details of 18 district police subdivisions that are subordinate to Dhaka Range, but a 2018 one states there are only 14. This may indicate that some subdivisions of the Dhaka Range were disbanded or placed under a different command structure. In this case, although the details of the source remain the same we have created two access points for it: the first is for the 2013 archive snapshot, the second for the 2018 one.
- *Access points based on page number*: in the 2015 report *Stars on their shoulders. Blood on their hands. War crimes committed by the Nigerian military* Human Rights Watch made a large number of allegations against the Nigerian Army. The report is 133 pages long. We have used information from specific pages to evidence specific data points about units, persons and incidents. For example, we use information on page 11 as evidence of the **Person**: Name field for “John A. H. Ewansiha”; material from page 24 supplements what we know about the **Unit**: Name for “Civilian Joint Task Force”. In total, we have created 13 access points for this single source.

Access points are a flexible concept that enable us to specify precisely the material that we have used to evidence data point.

12.3 Source: Research Comments

Description

Observations specific to the process of reviewing data in this row, including fixes, refinements and other suggestions.

Type of field

Text and numbers

Example of use

Source need archiving, How to extract full publication timestamp from post?,
Source should not be published because permission has not been given by the
resource owner

Spreadsheet column name

source:comments:admin

Shortcode

s_c_a

Sources

No

Confidence

No

Guidance on use

This is an administrative field specific to data created in spreadsheets. Staff Researchers use it to pass on feedback about the data in the row. This may include changes needed to specific fields, references to sources that the owner of the row might look at, and other observations that can improve the quality of the data. Data in this field are not intended for publication.

12.4 Source: Restricted

Description

Field indicating that the source should not be published on WhoWasInCommand, or distributed in any public product.

Type of field

Number, single entry

Example of use

1

Spreadsheet column name

source:restricted:admin

Shortcode

s_r_a

Guidance on use

If a source should not be published on WhoWasInCommand, or distributed in any public form, the Staff Analyst can indicate this by placing a 1 in the `Source: Restricted` field. The reasons for restricted publication of a source should be recorded in `Source: Research Comments`.

12.5 Source: External Archive

Description

A set of fields recording where a copy of the source can be found in external archives

Type of field

Text and numbers

Example of use

0E94AE36DA6FF03992A57FDDDBDF4728B609D0D7FE6EB019FA9F1B9B5B540D835

Spreadsheet column name

Presently, the two available field refer to an archive that provides a separate SHA256 hash of both the source's content and its metadata. These are labelled:

`source:external_archive_sha_content:admin` and `source:external_archive_sha_meta:admin`

Shortcode

`s_eac_a` and `s_eam_a`

Guidance on use

This is a dynamic field designed to enable interlinking between sources recorded in the format used by Security Force Monitor, and those in use in other collections.

12.6 Source: Access Point Unique Identifier

Description

A unique 32 character code assigned to each access point.

Type of field

Text and numbers

Example of use

1c03ec21-0fae-4243-9de6-686568afc2b8

Spreadsheet column name

`source:access_point_id:admin`

Shortcode

`s_id_a`

Guidance on use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs can be created easily using either installable or online tools, for example:

- Linux and OSX users: `uuidgen` command line tool.

- On the web: **‘UUID Generator<<https://www.uuidgenerator.net/version>>’**__.

The field is administrative, providing a reliable way to differentiate between different access points.

When a new access point is created directly in WhoWasInCommand, the platform automatically creates a UUID for that access point and stores it in this field. If a new accesspoint is created in a spreadsheet, the Staff Researcher must generate a unique identifying number for that person and copy it into the field `source:access_point_id:admin` for that specific access point. This manual, copy-and-paste step is a potential source of error and the Staff Researcher must be careful not to re-use a UUID.

Bulk updates made to WhoWasInCommand.com by spreadsheet import are based on the values in this field. For example, changes made in the row `a407be6a-28e6-4237-b4e9-307f27b1202e` in the spreadsheet will be applied to the access point with that UUID in WhoWasInCommand.

12.7 Source: Type

Description

Description of the media type of the source, such as “document”, “video” or “image”.

Type of field

Text and numbers, controlled, single entry

Example of use

`document, video, message, tweet, post`

Spreadsheet column name

`source:type`

Shortcode

`s_ty`

Guidance on use

Use this field to capture data about the source’s basic media type. The choice of values is defined in a controlled vocabulary.

12.8 Source: Title

Description

The name of the source, as stated on the source.

Type of field

Text and numbers

Example of use

`Stars on their shoulders. Blood on their hands. War crimes committed by the Nigerian military`

Spreadsheet column name

`source:title`

Shortcode

s_t

Guidance on use

Copy the exact title of the source as stated on the source itself. Where the title has multiple parts, such as a subtitle, also include that.

12.9 Source: Author

Description

The name(s) of the person(s) who authored, or otherwise created, the source.

Type of field

Text and numbers

Example of use

Osa Okhomina, Tom Moses, Tony Wilson; Tom Longley

Spreadsheet column name

source:author

Shortcode

s_a

Guidance on use

Use this field to record the given name and surnames of the persons who authored or otherwise created the source. Typically, this will be a byline containing one or more persons. Where more than one person is credited as the author/creator, use a semi-colon to separate the names.

If the source is a social media post, and the real name of the author/creator cannot be found, record the social media account identity.

Where the author/creator is an organization (e.g. Press Association, Reuters and agencies) do not enter this in `Source: Author` - this information will likely be included in `Source: Publication Name`.

12.10 Source: Source URL

Description

The first and original public online location of the source.

Type of field

URL

Example of use

<https://www.amnesty.org/en/documents/afr44/1657/2015/en/>

Spreadsheet column name

source:url

Shortcode

s_u

Guidance on use

The URL included here must be for the first and original public online location of the source.

Where possible, if a source is republished through a content sharing or syndication system, attempt to find the original location.

If you are accessing the source through a restricted or subscription-only gateway (such as LexisNexis or ProQuest), attempt to find the original public URL for a source rather than the URL generated by the gateway service.

12.11 Source: Creation Date and Time

Description

Date and time that the source was created.

Type of field

ISO 8601 timestamp, full or partial, UTC timezone (YYYY-MM-DDThh:mm:ssZ)

Example of use

2019-11-29T10:25:45Z, 2019, 2010-11-29

Spreadsheet column name

source:created_timestamp

Shortcode

s_ct

Guidance on use

Where available, record the date and time that the source was created. The field accepts full or partial values: at its simplest this is to the year, at its most comprehensive it can be to the second. A creation timestamp may not be available for a source - if this is the case, leave this field blank.

Where the timezone is indicated, convert the timestamp to UTC.

12.12 Source: Upload Date and Time

Description

Date and time that the source was uploaded to the online platform or service on which it is hosted.

Type of field

ISO 8601 timestamp, full or partial, UTC timezone (YYYY-MM-DDThh:mm:ssZ)

Example of use

2019-11-29T10:25:45Z, 2019, 2010-11-29

Spreadsheet column name

source:uploaded_timestamp

Shortcode

s_ut

Guidance on use

Where available, record the date and time that the source was uploaded to the online platform or service on which it is hosted. This may differ from the date of creation or publication. Upload timestamp information may not be available for source - if this is the case, leave the field blank.

The field accepts full or partial values: at its simplest this is to the year, at its most comprehensive it can be to the second.

Where the timezone is indicated, convert the timestamp to UTC.

12.13 Source: Publication Date and Time

Description

Date and time that the source was published on the online platform or service on which it is hosted.

Type of field

ISO 8601 timestamp, full or partial, UTC timezone (YYYY-MM-DDThh:mm:ssZ)

Example of use

2019-11-29T10:25:45Z, 2019, 2010-11-29

Spreadsheet column name

source:published_timestamp

Shortcode

s_pt

Guidance on use

Where available, record the date and time that the source was published to the online platform or service on which it is hosted. This may differ from the date of creation or upload. Although a timestamp for creation and upload dates and times may not be available, it is very likely that at least a publication date will be available for a source. Where a publication date is not available for a source, the timestamp of the earliest snapshot of the source in the Internet Archive should be recorded here.

The field accepts full or partial values: at its simplest this is to the year, at its most comprehensive it can be to the second.

Where the timezone is indicated, convert the timestamp to UTC.

12.14 Source: Access Date and Time

Description

Full date on which the Staff Researcher looked at the source or its access points.

Type of field

Date (YYYY-MM-DD)

Example of use

2019-02-20

Spreadsheet column name

source:access_point_access_date

Shortcode

s_apad

Guidance on use

When a Staff Researcher accesses an access point, they should record the full, exact date in this field. This data is a useful part of quality assurance processes, enabling us to re-visit sources at set points in time to assess whether they have been updated.

12.15 Source: Access Point Type

Description

The method by which an access point to a source has been created, such as by page or archive snapshot

Type of field

Text, controlled, single entry

Example of use

pages, frame, clip, archive

Spreadsheet column name

source:access_point_trigger

Shortcode

s_apt

Guidance on use

A source has at least one access point, but may have many. For example, if a source is a document we may draw information from a number of different pages (or ranges of pages). For each page or range of pages, we would create a new access point to the source. The field *Source: Access Point Type* tells us what method we have used to create the access point - in this case page. The number of the page or page range will be recorded in the field *Source: Access Point Trigger*.

Currently, there are six methods for creating an access point:

- *archive*: an archive snapshot of the source contains different content from the source, or from other snapshots.
- *page*: a page or range of page in a document source like a book or report.
- *line*: a line or range of lines in a line-numbered document like an interview transcript.
- *clip*: a passage from a video or audio source, comprising a start time and a stop time.
- *frame*: a single capture point from a video.
- *still*: an image captured from a video or interactive resource which does not correspond to a specific frame.

The range of access point types may extend as different media forms become available.

12.16 Source: Access Point Trigger

Description

Number or number range describing where in a source to find the exact content that comprises the access point.

Type of field

Number, number range

Example of use

11, 11-12, 11, 13, 11, 13, 14-19, 1:31-1:40

Spreadsheet column name

source:access_point_trigger

Shortcode

s_aptr

Guidance on use

This field is used to specify the exact content within a source that defines the access point. For example, if we want to create an access point at page 4 of a source then we would set the value in `Source: Access Point Type` to page and enter 4 in `Source: Access Point Trigger`. As noted in the documentation for `Source: Access Point Type` there are six ways to create an access point. These are listed below, along with the data type and format required to specify the exact content of the access point:

- `archive`: duplicate the value in `Source: Access Point Archive URL`
- `page`: Single page (1), single range of pages (1-2), combination of page and page ranges (1, 2-3, 4, 5-8)
- `line`: Single line (200), single range of lines (200-230), combination of line and line ranges (200-230, 236, 240-250)
- `clip`: Single range containing start and end time in the format `hh:mm:ss` (00:01:20-00:01:24)
- `frame`: a single capture point from a video in `hh:mm:ss` format (00:01:20)
- `still`: a direct link to SFM's hosting library to an image captured from a video or interactive resource for which we do not have a specific time frame. For example, a `still` would be the appropriate type of access point to create to enable us to use as evidence multiple views of an online database that didn't provide permalinks for queries.

The range of access point triggers may extend as different media forms become available.

12.17 Source: Access Point Archive URL

Description

URL of a snapshot of the source captured by the Internet Archive and hosted on its Wayback Machine.

Type of field

URL

Example of use

<https://web.archive.org/web/20150703120013/http://www.amnesty.org/en/documents/AFR44/043/2012/en/>

Spreadsheet column name

source:archive_url

Shortcode

s_au

Guidance on use

A source becomes usable by Staff Researchers when it has an access point. After entering the source's basic details (like `Source: Title`), the researcher then creates the first access point by specifying an Internet Archive snapshot to use for that source. If the source is not already archived in the Internet Archive, the research must create a new snapshot to use as the access point. Where snapshots for the source already exist in the Internet Archive, the Staff Researcher should find the snapshot that is earliest in time.

In the majority of cases, this will suffice. However, in some cases, we may need to specify more than one Internet Archive snapshot for the same source. The common reason for this is that the source content changes, but the basic details of the source do not. A good example of this is this (dead) URL published by the *Secretaría de la Defensa Nacional* in Mexico: `http://www.sedena.gob.mx:80/ejercito/comandancias/gur_mil.htm`. It lists the commanders of Mexico's military garrisons, and we have included reference to this in our data. The title, initial publication date, publication and basic URL did not change; however, the content did. In each of 24 different captures made by the Internet Archive, the list of commanders is different. In this case, we have a single source with 24 access points: each access point refers to a specific version of that source containing the exact information that we relied upon to create the data.

The example above also illustrates an important point: sometimes a source is only available in an archived form, because its original source URL is no longer online. There are many reasons a link may no longer be live, and this problem is known as "linkrot". In these cases, the Staff Researcher can fill in `Source: URL` with a portion of the Internet Archive URL printed after the timestamp:

```
https://web.archive.org/web/20040208204841/http://www.sedena.gob.mx:80/
ejercito/comandancias/gur_mil.htm
```

12.18 Source: Access Point Archive Timestamp

Description

Timestamp of the Internet Archive snapshot used to create an access point.

Type of field

Date (YYYY-MM-DDTHH:MM:SS)

Example of use

2004-02-08T20:48:41

Spreadsheet column name

source:access_point_archive_timestamp

Shortcode

s_apat

Guidance on use

Every snapshot made by the Internet Archive contains a timestamp of the time (GMT/UTC) when that snapshot was created. The timestamp is contained in the URL and looks like this:

20040208204841

We extract this part of the URL and reformat it to something more human readable (an ISO 8601 format):

2004-02-08T20:48:41

The timestamp is a useful quality assurance filter, and is used in the WhoWasInCommand data entry tools as a visual aid to differentiate between access points.

12.19 Source: Publication Country

Description

Country in which the publication or publishing organization of the source is based.

Type of field

Text, controlled vocabulary

Example of use

United States, Nigeria

Spreadsheet column name

source:publication_country

Shortcode

s_c

Guidance on use

Values for this field are the English language full names of countries contained in the list of ISO 3166-1 alpha-2 codes, which can be found ([on the ISO website](#) and on [Wikipedia](#)).

12.20 Source: Publication Name

Description

The name of the publication, or publishing organization, of the source.

Type of field

Text

Example of use

Amnesty International, Secretaría de la Defensa Nacional, Daily Independent, The Irrawady

Spreadsheet column name

source:publication_title

Shortcode

s_pt

Guidance on use

This field can cover two sorts of publication:

- The publication in which the source appears, which could be a newspaper, journal or a book.
- Absent a specific publication, include the name of the publishing organization, such as the government organization responsible for a web-page.

12.21 Source: Publication Unique Identifier

Description

A unique 32 character code assigned to each publication from which sources are drawn.

Type of field

Text and numbers

Example of use

2190a9b4-8163-47a6-8461-3157f68c3ba3

Spreadsheet column name

source:publication_id:admin

Shortcode

s_pid_a

Guidance on use

This value is a Universally Unique Identifier (UUID) generated using a computer program. UUIDs can be created easily using either installable or online tools, for example:

- Linux and OSX users: *uuidgen* command line tool.
- On the web: **‘UUID Generator<<https://www.uuidgenerator.net/version>>’**__.

The field is administrative, providing a reliable way to differentiate between different publications (which in some cases may have the same name).

When a new publication is created directly in WhoWasInCommand, the platform automatically creates a UUID for that source and stores it in this field. If a new publication is created in a spreadsheet, the Staff Researcher must generate a unique identifying number for that publication and copy it into the field `publication:id:admin` for every row associated with that specific publication. This manual, copy-and-paste step is a potential source of error and the Staff Researcher must be careful not to re-use a UUID.

Frequently Asked Questions about WhoWasInCommand

13.1 What is WhoWasInCommand?

In short: a search engine about security forces, their structures, personnel, areas of operation and connections to allegations of human rights abuses.

Longer version:

WhoWasInCommand answers key questions about the structure, behaviour and people in charge of security forces like the police and army:

- Who is in charge of the specialized anti-riot police unit?
- What army unit has jurisdiction over what areas and for how long?
- Where did this commander previously serve, and where did they go next?
- When was a particular police unit based in a specific city?
- What allegations have civil society groups made against a unit or commander?

WhoWasInCommand presents data from thousands of public sources to help human rights researchers, investigative journalists and anyone who wants security forces to be more accountable.

13.2 How do I find what I'm looking for?

Got this page?

When you enter a search term into WhoWasInCommand, it will search across 28 different fields that contain text to attempt to find a match for your term. Where it can't find a match, it will alert you. If find a term that is a bit like the term you are searching, WhoWasInCommand may make a suggestion to you.

Use a combination of search terms and different filters to see what sets of results appear, and gradually refine it until you find what you are looking for.

Go!

No results found for “Why aren't any results showing?”

For better results, try adjusting your search filters.

Think we're missing something? [Let us know!](#)

You can also use our “Countries” page as a jump-off point. It has direct links to all the units, person and incidents for a particular country, along with some “collections” we have added.

13.3 Where can I find help understanding what I’m seeing or how this website works?

On WhoWasInCommand you will see lots of little question marks. Click on them to be taken to a page describing what the data means, or how a particular feature of the website works.

A tool from [Security Force Monitor](#)

WhoWasInCommand

[Countries](#)
[Personnel](#)
[Units](#)
[Incidents](#)
[Help](#)
[About](#)
English

21 Armoured Brigade ? [Download as CSV](#) [Print this page](#)

Also known as: 21 Brigade | 21-Armoured Brigade | 21 Armored Brigade

Country: **Nigeria**

Classified as: **Military Army**

[Contents ?](#)
[Areas of operation ?](#)

[Areas of operation](#)
[Sites](#)
[Memberships](#)

13.4 Where can I find out more about the data on “units”, “persons” and “incidents”?

Visit the help pages for that specific type of record:

- For “units” visit [Unit Records on WhoWasInCommand](#)
- For “persons” visit [Person records on WhoWasInCommand](#)
- For “incidents” visit [Incident Records on WhoWasInCommand](#)

If these do not answer your question, please write to us at technical@securityforcemonitor.org and we’ll help out.

13.5 How can I see all the units for a particular country?

The quickest way to do this is:

- Select “Units” from the navigation bar at the top of WhoWasInCommand, which will list every unit in the database
- Then, on this search results page open “General Filters”, choose “Country” and select from that list
- The results will then be filtered for that country.

13.6 Why does WhoWasInCommand make suggestions to me?

It’s trying to be helpful. When you enter a search term and WhoWasInCommand does not make an exact match, it may present words that have some degree of similarity, or sound similar. For example, searching with the term `operat` causes WhoWasInCommand to suggest that you might be searching for an `operation`:

Go!

1 result found for “operat”

Did you mean: [Operación Chihuahua](#) | [Operación "CHIHUAHUA"](#) | [Operación Conjunta](#) | [Operación Conjunta Chihuahua](#) | [Operación Conjunta Culiacán-Navolato-Guamúchil-Mazatlán](#) | [Operación Conjunta Nuevo León – Tamaulipas](#) | [Operación Coordinada Chihuahua](#) | [Operación Guerrero Seguro](#) | [Operación Interinstitucional Culiacán-Navolato](#) | [Operación Noreste](#)

13.7 How do I see the sources used for a specific datapoint?

Let’s say you are interested in the sources used to link a person to an organization:

Memberships

Organization	Rank	Role	Title	First cited	Last cited
35 Batallón de Infantería	Coronel	Commander		<u>18 October 2009</u>	<u>19 January 2010</u>

Hover your mouse (or tap on it, if on a tablet or mobile) over any of the values and little coloured circle will appear:

Memberships

Organization	Rank	Role	Title	First cited	Last cited
35 Batallón de Infantería ⁵	Coronel	Commander		<u>18 October 2009</u>	<u>19 January 2010</u>

Click it to see a little “pop-over” that lists all the sources for that datapoint:

3 sources for this datapoint ×
Confidence: LOW

Title: “Sentencian a 33 años de prisión a mandos militares por asesinato de dos civiles”
Publication: Proceso
Published on: 2016-01-21
Source URL:
<http://www.proceso.com.mx/427171-a-33-anos-de-prision-a-mandos-militares-por-homicidio-de-dos-civiles>

Organization	Rank	Role	Title	First cited	Last cited
35 Batallón de Infantería ⁵	Coronel	Commander		<u>18 October 2009</u>	<u>19 January 2010</u>

This pop-over shows you the number of sources for the datapoint. You can scroll up and down to see them, and click on the links to access the sources directly. It also shows you the confidence rating that we have given the specific datapoint.

13.8 What are those little numbered circles that keep appearing?

You mean these?

The little numbered circles indicate two things: * Click on it to show a list of the sources used to evidence that specific datapoint. * The colour indicates the level of confidence we have in the data: Red for “Low”, yellow for “Medium” and green for “High”. You can read an explanation of how we grade information in this handbook’s page on [Data integrity measures](#).

13.9 Why do some dates have a dotted line beneath them and some don’t?

If there is a dotted line under a date, this means that we think this is an exact start date or exact end date. This means that a source has been very specific about the date when, for example, a unit was created or started operating in an area.

If there is no dotted line under a date, this indicates that it is just the earliest reference we have for the creation of a unit, or the commencement of an operation.


Area	First cited	Last cited
Buenaventura	29 December 2009	
Nuevo Casas Grandes	25 September 2009	29 December 2009
Delicias	30 July 2009	

13.10 The command chart is taking a looooong time to load. Is there a problem?

Probably not, but if it keeps happening to you report it to us at technical@securityforcemonitor.org.

There can sometimes be a short delay between loading a page and the appearance of the Chain of Command or Parent Unit chart. When this is happening, we display a “spinner” to let you know. It looks like this:

Parent units

All units that have held a command position over this unit. 

Swipe to zoom, click and drag to pan



Unit Records on WhoWasInCommand

This page gives an overview of the data that visitors to WhoWasInCommand will find in a unit record.

This includes descriptions of different sections of the unit page, the data fields that are used to create it and links to more information about each field.

14.1 Unit record: Title area

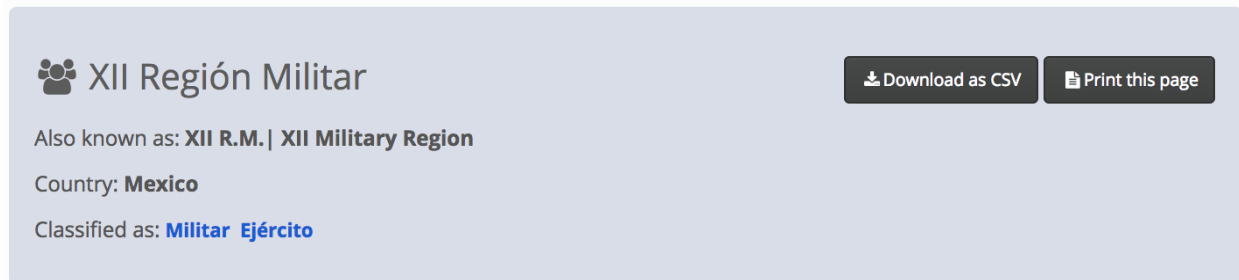


Fig. 1: Image showing the title area of an unit record on WhoWasInCommand

This section contains key information about the identity of the unit. It also contains links to download and print actions for the displayed record. Hover over any value in the unit title area to display a little coloured circle; clicking on this will display the sources and confidence rating for each value.

Fields used in the unit record title area

The following fields are used in the title area:

- *Unit: Name*
- *Unit: Other Names*
- *Unit: Classification*

- *Unit: Country*

When a field is empty, it will not be displayed in the Title area.

14.2 Unit record: Content sidebar

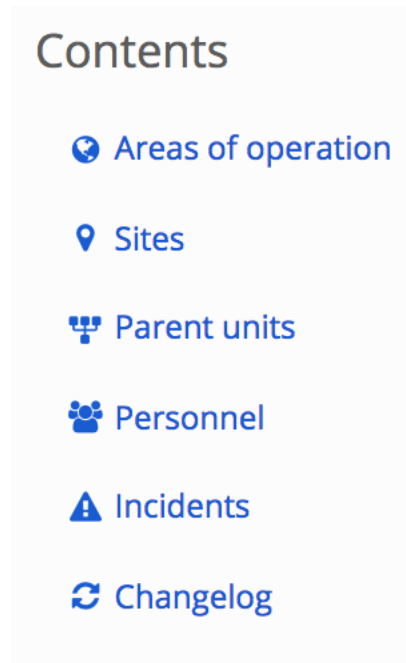


Fig. 2: Image showing the content sidebar of an unit record on WhoWasInCommand

The content sidebar is a navigation aid. It provides quick links to different parts of the page. The items inside the content sidebar indicate what sort of data is available about this unit. For example if “Incidents” is not listed in the content sidebar, then there is no data available about incidents involving this unit.

14.3 Unit record: Areas of Operation

The areas of operation section contains a map and table that describe where an organization has operated in some manner. Click on the highlighted areas of the map to display the name of an area of operation. Grab the map to drag/pan it around. Swipe or use the + and – controls on the map to zoom in or zoom out. Hover over any value in the table and a little coloured circle will appear. Click on this to view the sources and confidence rating we have assigned to that value.

The Areas of Operation section will display where an area of operations has been specified, otherwise it will not appear.

14.4 Unit record: Sites

This section contains a map and a table that describe sites associated with the organization. Clicking on the pins plotted on the map will display the name of the site. Grab the map to drag/pan it around. Swipe or use the + and –

Areas of operation



Area	First cited	Last cited
Querétaro	February 1999	5 July 2016
Michoacán de Ocampo	February 1999	25 August 2016
Guanajuato	February 1999	2 December 2016

Fig. 3: Image showing the Area of Operations map and table of a unit record on WhoWasInCommand.com

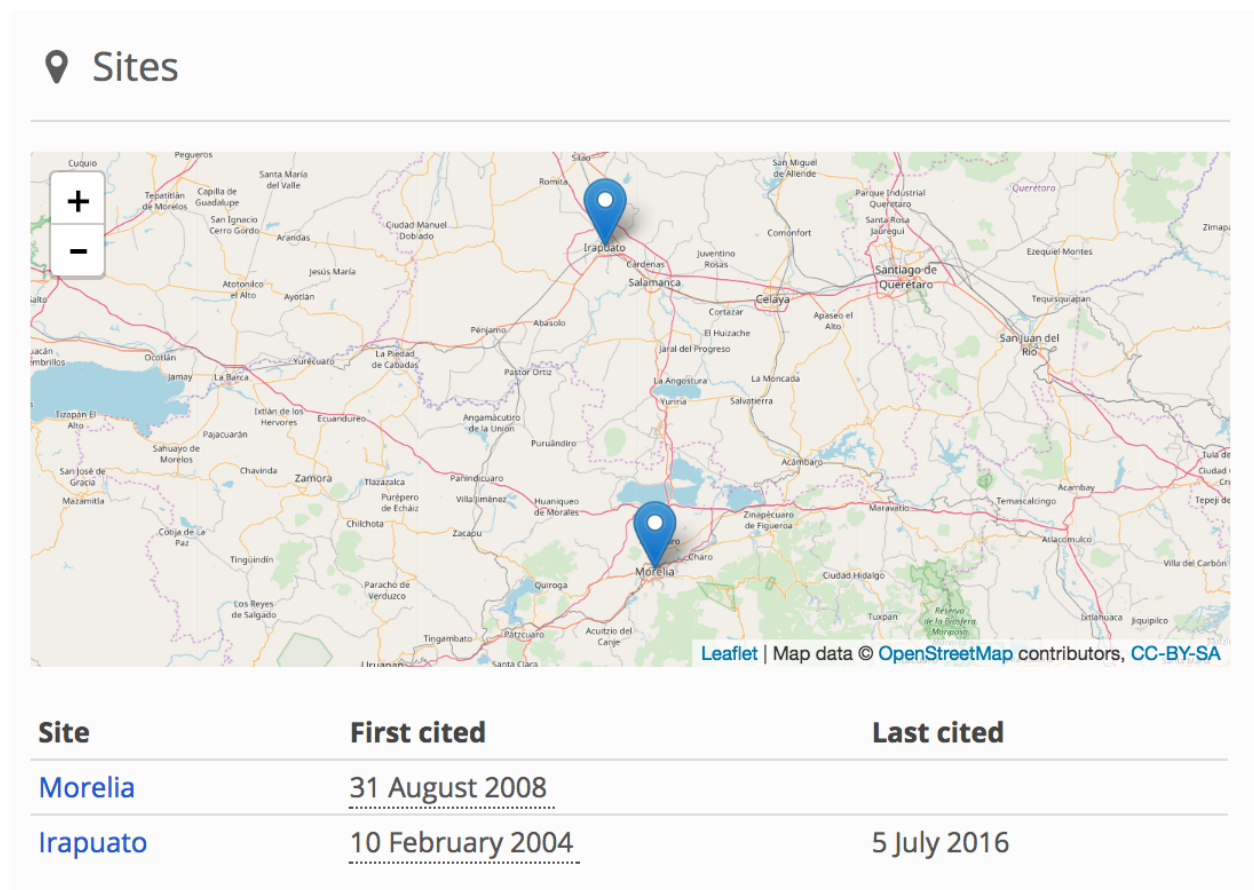


Fig. 4: Image showing a map and table of sites - or bases - as part of an unit record on WhoWasInCommand.com

controls on the map to zoom in or zoom out. Hover over any value in the table and a little coloured circle will appear. Click on this to view the sources and confidence rating for that value.

The Sites section will display where there is a valid site record. Otherwise, the section will not display on the unit record.

14.5 Unit record: Memberships

Memberships Multi-unit organizations that this unit is part of

Name	Aliases	Classifications	First cited	Last cited
Operativo Conjunto Michoacán			16 January 2010	29 December 2010

Fig. 5: Image showing a membership table of a unit record on WhoWasInCommand.com

This section contains a table indicating whether the organization has been a member of internal/national joint operations, international peacekeeping missions, or other multi-unit deployments. Hover over any value in the table and a little coloured circle will appear. Click on this to view the sources and confidence rating for that value.

Where a unit has no memberships attached to it, the memberships section will not display on the unit record.

14.6 Unit record: Member units

Member units

Name	Aliases	Classifications	First cited	Last cited
103 Battalion	103 BN	Military Army	2009	
146 Battalion	146 Mechanised Battalion	Military Army	8 October 2007	
174 Battalion	174 Mechanised Battalion 174 Bn	Military Army	2009	
19 Battalion	19 BN 19BN	Military Army		1 November 2011
192 Battalion	192 Motorised Battalion	Military Army	2013	

This section contains a table listing the units that comprise the present unit. For example, it will list units that have taken part in a joint operation, international peacekeeping mission or other multi-unit organization. However over any

value in the table, and a little coloured circle will appear. Click on this to view the sources and confidence rating for that value.

14.7 Unit record: Parent units



Fig. 6: Image showing a table of parent units for an organization on WhoWasInCommand.com

The parent units section displays an interactive chart. This shows the links between all units known to be above the present one in the overall organizational hierarchy of that security force, right up to the Commander in Chief or equivalent. The chart is drawn using parent relationships that are classified as `command` (rather than `informal` or `administrative`). They are drawn at the last cited or end date of the parent relationship. This date is displayed at the bottom of the chart. Where a unit has different parents at different times, a chart is drawn for each relationship: swiping left or right, or using the arrows at each side, displays these.

Where a unit does not have a parent relationship, this section will not be displayed in the unit record.

14.8 Unit record: Unit subsidiaries

The subsidiaries section contains a table describing all units known to have been immediately below the current unit in the overall organizational hierarchy of that security force. Hover over any value in tables to display a little coloured circle; clicking on this will display the sources and confidence rating for each value.

Fields used in the Unit subsidiaries section

Where a unit has no subsidiaries, this section will not be displayed in the unit record.

Subsidiaries

Name	Aliases	Classifications	First cited	Last cited
16 Zona Militar	16/a. Z.M. 16/a. ZM 16/a. 16/a. Zona Militar	Militar Ejército	10 February 2004	9 January 2017
17 Zona Militar	17/a. Z.M. 17/a. ZM 17/a. 17/a. Zona Militar	Militar Ejército	10 February 2004	21 November 2016
21 Zona Militar	21/a. Zona Militar XXI Zona Militar 21/a Z.M. 21/a. Z.M. 21/a. ZM 21/a.	Militar Ejército	10 February 2004	9 January 2017
43 Zona Militar	43/a. Zona Militar 43 Military Zone zona número 43 43/a. Z.M. 43/a. ZM 43/a. 43/a Z.M.	Militar Ejército	30 January 2000	9 January 2017

Fig. 7: Image showing a table of subsidiaries on an unit record on WhoWasInCommand.com

14.9 Unit record: Unit personnel



Personnel Table showing personnel linked to this unit in command, administrative and other roles

Name	Rank	Role	First Title cited	Last cited
Amado Onésimo Flores Morales	General de Brigada	Jefe de los Servicios Regionales	30 July 2010	18 October 2010

Fig. 8: Image of a table showing a list of personnel on an organization record on WhoWasInCommand.com

The personnel section displays a table showing all persons affiliated to this unit at any time in command, administrative and other roles. Hover over any value in the table to display a little coloured circle; clicking on this will display the sources and confidence rating for each value.

Fields used in the unit personnel section

Where no persons in the dataset are members of a unit, this section will not be displayed in the unit record.

14.10 Unit record: Unit incidents



Incidents

Incident on 11 July 2006

According to Comisión Nacional de los Derechos Humanos: "Siendo aproximadamente las 01:05 horas del 11 de julio de 2006, en el salón denominado "El Pérsico Dancing", un civil de sexo masculino estaba alterando el orden del lugar y causando problemas a uno de los clientes, por lo que fue detenido ...

Fig. 9: Image showing a list of incidents on an unit record on WhoWasInCommand.com

The incidents section displays a list of incidents of alleged human rights violations that sources allege the unit has committed. Hover over either the date or the incident description to display a little coloured circle that when clicked will show the sources and confidence rating we have assigned to this data.

Fields used in the unit incidents section

If a source has not made an allegation against a unit, this section will not be displayed in the unit record.

Person records on WhoWasInCommand

This page contains an overview of the data that visitors to WhoWasInCommand will find in a person record.

This includes the different sections of the person record, the data fields that are used to create it and links to more information about each field.

15.1 Person record: Title area

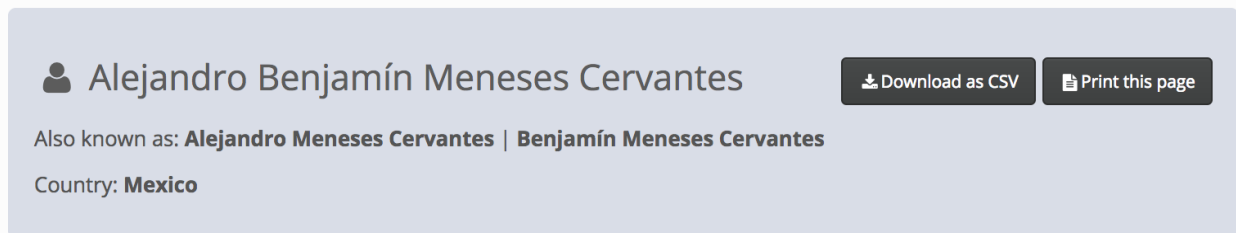


Fig. 1: Image showing the title area of a person record on WhoWasInCommand.com

This section contains key information about the identity of the person. It also contains links to download and print actions for the displayed record. Hover your mouse or tap any value in the title area and a little coloured circle will appear: click this to display the sources and confidence rating that we have assigned to that datapoint.

15.2 Person record: Content sidebar

The content sidebar is a navigation aid. It provides quick links to different sections of the person record. The items inside the content sidebar indicate what sort of data is available about this person. If a particular section is not listed in the content sidebar - for example, “Subordinates” - then there is no data available about the subordinates of this person.

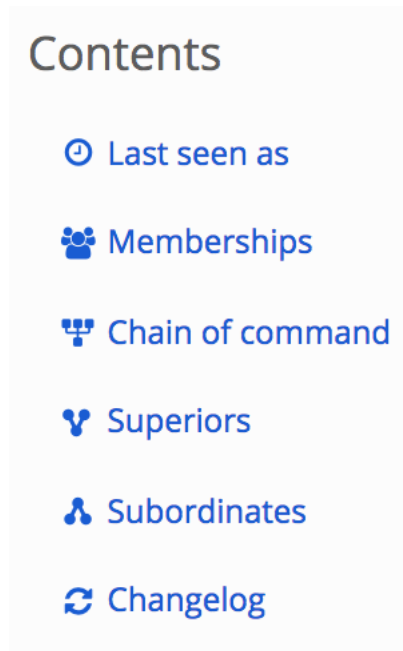


Fig. 2: Image showing the content sidebar of a person record on WhoWasInCommand.com

15.3 Person record: Person “Last Seen As”

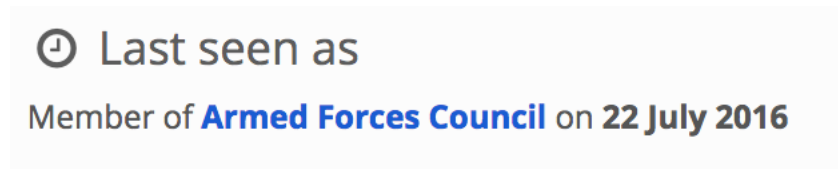


Fig. 3: Image showing the Last Seen As section of a person record on WhoWasInCommand.com

This section summarises the most recently-available data about a person’s rank, role and membership of a unit. Hover over any value in this section and a little coloured circle will appear. Click on this to view the sources and confidence rating for that value.

15.4 Person record: Person memberships

This section contains a table that describes the positions a person has held in different units. In this table, WhoWasInCommand will display a new membership row is displayed for each time a person changes unit, rank, role or title. This means that in some records a person may have multiple memberships in the same organization, but in different roles or at a different rank.

As with all tables in person, unit and incident records on WhoWasInCommand, hovering over or tapping any value in the table will cause a little coloured circle to appear. Clicking or tapping again on this will show the sources and confidence ratings we have assigned to that value.

Memberships

Organization	Rank	Role	Title	First cited	Last cited
Armed Forces Council				4 August 2015	22 July 2016
Nigerian Army	Lieutenant General	Commander	Chief of Army Staff	4 August 2015	5 August 2017
Nigerian Army Headquarters	Lieutenant General	Commander	Chief of Army Staff	4 August 2015	5 August 2017
2 Amphibious Brigade	Major General	Commander		19 December 2012	31 January 2013
Joint Task Force, Operation Pulo Shield, Sector 2	Brigadier General	Commander		7 May 2012	31 January 2013
2 Amphibious Brigade	Brigadier General	Commander		2 July 2011	18 December 2012

Fig. 4: Image showing the memberships table on a person record on WhoWasInCommand.com

15.5 Person record: Chain of command

The chain of command section displays interactive charts. These show the links between all the units commanded by a person and all those superior to them, along with their commanders. The chart will display up to the highest-level unit in the unit structure, creating a “line of sight” from the current unit to the top.

The charts are drawn using parent relationships between units that are classified as `command` (rather than `informal` or `administrative`). You can learn more about this in the documentation for *Unit: Related Unit Classification*.

The charts are drawn at the last cited or end date of the parent relationship. This date is displayed at the bottom of the chart. Where a unit has different parents at different times, a chart is drawn for each relationship: swiping left or right, or using the arrows at each side, displays these.

15.6 Person record: Superiors

This section displays a table of commanders of units that were superior to any units commanded by this person, along with the duration of overlap in service that sources are able to evidence. As with all tables in person, unit and incident records, hovering over or tapping any value in the table will cause a little coloured circle to appear. Click or tap again on this to view the sources and confidence ratings we have assigned to that value.

The below fields are calculated from the date values in the above fields:

- *Start of overlap*: the earliest date that the present person and a commander of an immediately superior unit served at the same time.
- *End of overlap*: the last date that the present person and a command of an immediately superior unit served at the same time.
- *Duration of overlap*: the number of days the present person and an immediate superior served at the same time.

Chain of command

Command relationships from a person's posting to the highest-level unit (calculated at the end of the posting)

Swipe to zoom, click and drag to pan



Fig. 5: Image showing the Chain of Command interactive chart that appear on person records on WhoWasInCommand.com

Superiors

Commanders of units that were superior to any units commanded by this person

Name	Rank	Role	Unit	Start of overlap	End of overlap	Duration of overlap
Abdul Hafeez Adewuyi	Major General	Commander	82 Division	13 October 2004	Unknown	Unknown
Rafiu Adeshina	Major General	Commander	82 Division	27 April 2004	Unknown	Unknown
Abdul Hafeez Adewuyi	Major General	Commander	82 Division	13 October 2004	Unknown	Unknown
Rafiu Adeshina	Major General	Commander	82 Division	27 April 2004	Unknown	Unknown

Fig. 6: Image showing the table of commanders of superior units that appears on a person record on WhoWasInCommand.com

15.7 Person record: Subordinates

Subordinates

Commanders of units that were subordinate to any units commanded by this person

Name	Rank	Role	Unit	Start of overlap	End of overlap	Duration of overlap
Adeniyi Oyabade	Major General	Commander	1 Mechanised Division	29 July 2015	6 August 2017	739 days
Kasimu Abdulkarim	Major General	Commander	6 Division	11 September 2016	2 February 2017	144 days
Ahmad Jibrin	Major General	Commander	2 Mechanised Division	6 September 2013	Unknown	Unknown
Chukwunedum Abraham	Major General	Commander	2 Mechanised Division	26 July 2017	Unknown	Unknown
Mohammed Sani Ali	Brigadier General	Commander	3 Armoured Division	26 January 2016	Unknown	Unknown
Enobong Okon Udoh	Major General	Commander	6 Division	3 February 2017	Unknown	Unknown
Tamunomeibi Dibi	Major General	Commander	81 Division	30 April 2015	Unknown	Unknown
Ebenezer Oyefolu	Major General	Commander	81 Division	25 April 2017	Unknown	Unknown
Oyefesobi	Lieutenant Colonel	Commander	6 Battalion	17 October 2007	Unknown	Unknown
Oyefesobi	Lieutenant Colonel	Commander	6 Battalion	17 October 2007	Unknown	Unknown

Fig. 7: Image showing the table of subordinate personnel that appears on person records on WhoWasInCommand.com

This section displays a table of commanders of units that were subordinate to any units commanded by this person. As with all tables in person, unit and incident records on WhoWasInCommand, hovering over or tapping any value in the table will cause a little coloured circle to appear. Click or tap again on this to view the sources and confidence ratings we have assigned to that value.

Fields used in the person subordinates section

The following fields are calculated from date values in the above fields:

- *Start of overlap*: the earliest date that the present person and a commander of an immediately subordinate unit served at the same time.
- *End of overlap*: the last date that the present person and a command of an immediately subordinate unit served at the same time.
- *Duration of overlap*: the number of days the present person and an immediate superior served at the same time.

Incident Records on WhoWasInCommand

This page contains an overview of the data that visitors to WhoWasInCommand will find in an incident record.

This includes the different sections of the incident record, the data fields that are used to create it and links to more information about each field.

16.1 Incident record: Title area



The screenshot shows a light blue rectangular box representing the title area of an incident record. At the top left is a warning icon (an exclamation mark inside a triangle). To its right is the text "Incident between 21 October 2008 and 26 October 2008". To the right of this text are two dark grey buttons: "Download as CSV" with a download icon and "Print this page" with a printer icon. Below the main title, the text "Country: Mexico" is displayed. At the bottom of the box are two dark grey buttons: "Torture" and "Illegal detention".

This section contains key information about the incident. It also contains links to download and print actions for the displayed record. Hover over any value in the title area to display a little coloured circle; clicking on this will display the sources and confidence rating for we have assigned to each value.

16.2 Incident record: Content sidebar

The content sidebar is a navigation aid. It provides quick links to different sections of the record. The items inside the content sidebar indicate what sort of data is available about this incident. For example if “Perpetrator units” is not

Contents

 Location

 Description

 Perpetrator
organizations

 Changelog

listed in the content sidebar, then there are no data available about alleged perpetrators of the incident.

16.3 Incident record: Location

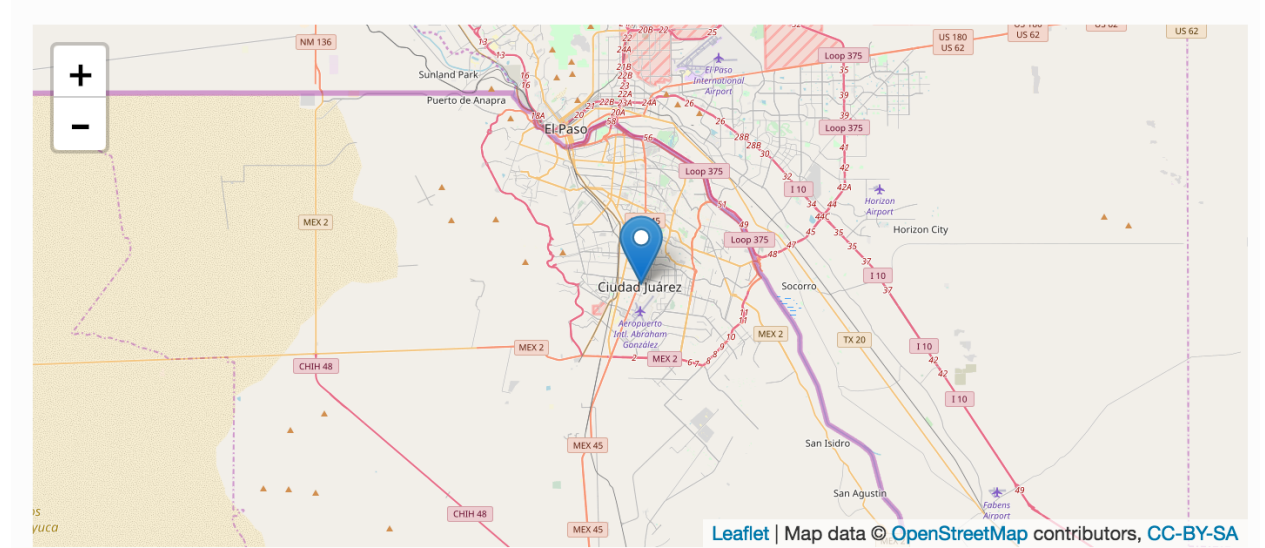
This section contains an interactive map and some text that describe the location where sources indicate that an incident occurred. Click on the pins placed in the map to display the name of a location. Grab the map to drag/pan it around. Swipe or use the + and – controls on the map to zoom in or zoom out. Hover over the text description of the location and a little coloured circle will appear. Click on this to view the sources and confidence rating we have assigned to that value.

16.4 Incident record: Description

This section contains a direct quotation from the civil society, governmental or other source that describes the incident. As with all tables in person, unit and incident records on WhoWasInCommand, hovering over or tapping any value in the table will cause a little coloured circle to appear. Clicking or tapping again on this will show the sources and confidence ratings we have assigned to that value.

16.5 Incident record: Perpetrator units

This section contains a table listing the unit(s) that sources allege committed the human rights violation(s) described in the incident. As with all tables in person, unit and incident records on WhoWasInCommand, hovering over or tapping any value in the table will cause a little coloured circle to appear. Clicking or tapping again on this will show the sources and confidence ratings we have assigned to that value.



This incident took place in **Mexico**

According to Amnesty International: "On 21 October 2008, 31 year-old Saúl Becerra Reyes and five other men were arrested by soldiers in a car-wash near the home he shared with Brenda Patricia Balderas and their two children in Ciudad Juárez, Chihuahua state. After being tortured and held illegally for five days by the military at the barracks of 20th Motorized Cavalry Regiment, five of the detainees were transferred on 26 October to PGR detention and charged with drug and firearm offences."

[Show less](#) ↑



Perpetrator organizations

Name	Aliases	Classification
20 Regimiento de Caballería Motorizado	20 Batallón de Caballería Motorizado 20/o. R.C.M. 20/o. Regimiento de Caballería Motorizado 20 Regimiento de Caballería Motorizada Vigésimo Regimiento de Caballería Motorizada 20° Regimiento de Caballería Motorizado Segundo Regimiento de Caballería Motorizado XX Regimiento de Caballería Motorizada 20/o. RGTO. CAB. MTZ. 20/o. RGTO. DE CAB. MOTORIZADO	Militar Ejército

What data can I download from WhoWasInCommand?

Note: May 2022: The WhoWasInCommand.com download feature is experimental and subject to change. Currently, the downloads do not reflect improvements in how the Security Force Monitor data model deals with Locations.

17.1 Data for download

Any data published on WhoWasInCommand can be downloaded as a set of Comma Separated Values (.csv) files. These can be easily loaded into a spreadsheet or database tool for analysis. To use WhoWasInCommand's data download feature visit the following link:

<https://whowasincommand.com/en/download>

The Security Force Monitor data model is a directed graph containing attributes about units, persons, locations as they change across time. This is quite complicated and does not easily translate into a single file that is straightforward to understand and use without guidance. To get around this and provide a way to provide raw data directly to users, we offer seven different reports drawn from the data on a specific country:

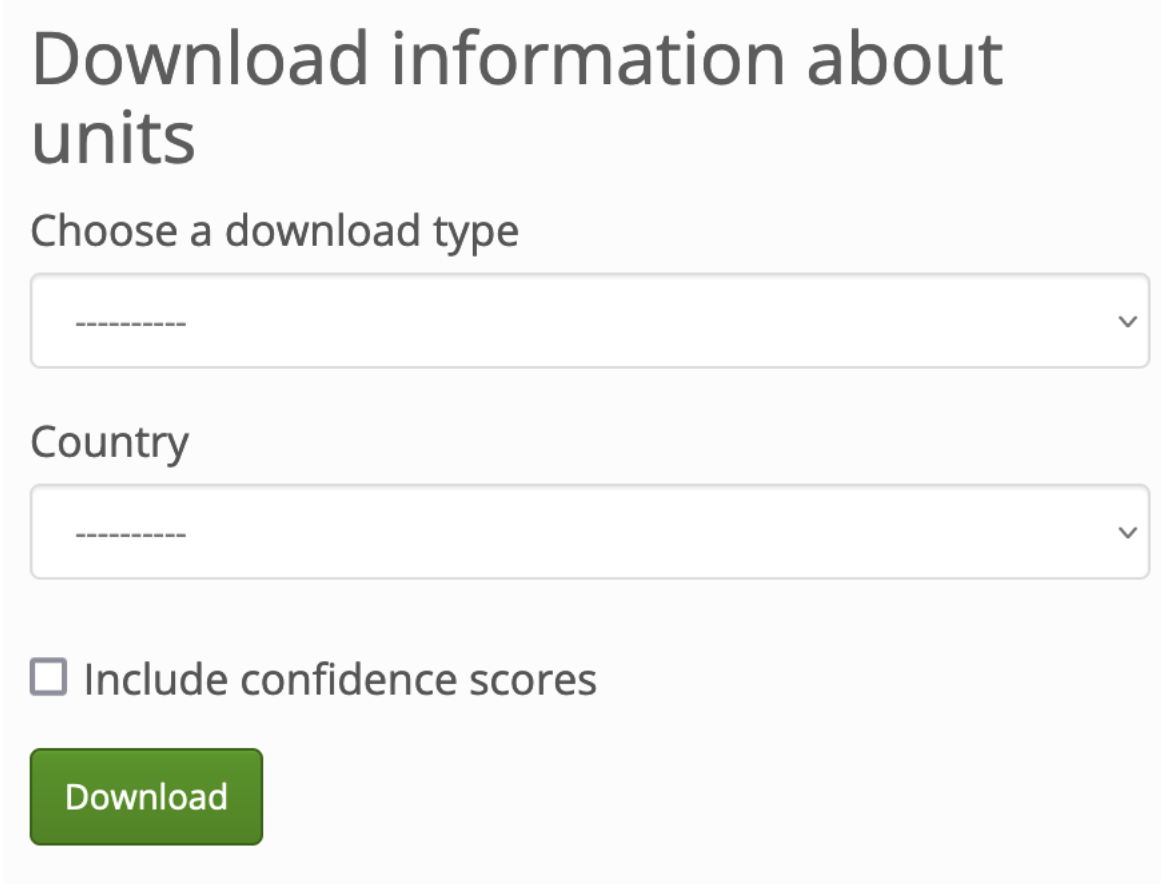
- **Basic:** a list of all the units in that country.
- **Parentage:** units organized into a hierarchy.
- **Memberships:** units that are part of operations that may fall outside the regular chain of command.
- **Areas of operation:** geographical distribution of units' operational areas.
- **Sites:** specific locations.
- **Personnel:** list of command personnel.
- **Sources:** sources used to evidence the data.

A full description of each downloadable slice of data is available in the sections below. It is important to note that none of the download contain the field-level sourcing that is a key part of Security Force Monitor's work (see the Research Handbook section on *Data integrity measures* for more information). The reason for this is technical (discussed [here](#)) on the code repository for the software that powers WhoWasInCommand.

17.2 How to download

Visit the download page: <https://whowasincommand.com/en/download>

The interface looks like this:

The screenshot shows a web form titled "Download information about units". It contains two dropdown menus: "Choose a download type" and "Country", both with dashed lines indicating they are empty. Below these is a checkbox labeled "Include confidence scores" which is currently unchecked. At the bottom is a green button labeled "Download".

Download information about units

Choose a download type

Country

☐ Include confidence scores

Download

Use the dropdown menu to select the report that you want to download:

Then, use the next dropdown menu to choose the country about which you want to download data:

Optionally, tick the checkbox to include Confidence Scores in the downloaded report. Read the page on [Confidence scores](#) for more information about this data integrity measure. As mentioned above, downloads do not currently include field-level sourcing.

Finally, click "Download" and a file containing the report will be downloaded to your computer. To help you identify the report, its filename is created using this simple template: `[report_type]_[country]_[YYYY-MM-DD].csv`

17.3 Contents of each download

In this section we outline the seven different slices of data that users can download from WhoWasInCommand.com.

Download information about units

Choose a download type

✓ -----

Basic

Parentage

Memberships

Areas of operation

Sites

Personnel

Sources

Download

Download information about units

Choose a download type

Basic



Country

Mali



☐ Include confidence scores

Download

17.3.1 Download: Basic

Description

The “Basic” download contains a list of distinct units in the dataset, along with force branch, aliases, earliest and latest observation dates for each unit.

Fields

- unit:id:admin
- unit:name
- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open

17.3.2 Download: Parentage

Description

The “Parentage” download contains data that describes how units fit into the organizational structure of the security and defence forces of the specified country. Each row contains a child-parent (`unit:name` - `unit:related_unit`) relationship inside the organizational hierarchy. Each row also contains data on the timescale for each relationship. You can find more information about how relationships between units work in the *Unit: Related Unit* section of this handbook.

Fields

- unit:id:admin
- unit:name
- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open
- unit:related_unit
- unit:related_unit:name
- unit:related_unit:country
- unit:related_unit_class
- unit:related_unit_first_cited_date

- unit:related_unit_first_cited_date_start
- unit:related_unit_last_cited_date
- unit:related_unit_open

17.3.3 Download: Memberships

Description

The “Memberships” download contains data showing that the unit has been attached to internal/national joint operations, international peacekeeping operations, or other multi-unit efforts. These operational unit groupings exist in parallel to units’ positionings in the regular organizational structure as described in the “Parentage” download. You can find more information about how memberships work in the *Unit: Related Unit* section of this handbook.

Fields

- unit:id:admin
- unit:name
- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open
- unit:membership_id
- unit:related_unit
- unit:member_country
- unit:member_classification
- unit:related_unit_first_cited_date
- unit:related_unit_first_cited_date_start
- unit:related_unit_last_cited_date
- unit:related_unit_open

17.3.4 Download: Areas of operation

Description

The “Areas of operation” download describes the geographical areas that units have either been assigned to or in which they have been observed operating within. The Research Handbook sections *Unit: Location Type*, *Unit: Location* and *Locations* describe the concept of an area of operation in more detail.

Fields

- unit:id:admin
- unit:name

- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open
- unit:area_ops_id
- unit:area_ops_name
- unit:area_ops_country
- unit:area_ops_feature_type
- unit:area_ops_admin_level
- unit:area_ops_admin_level_1_id
- unit:area_ops_admin_level_1_name
- unit:area_ops_admin_level_2_id
- unit:area_ops_admin_level_2_name

17.3.5 Download: Sites

Description

The “Sites” download describes the specific locations at which specific units have been observed. This download covers locations like infrastructure (such as police stations, barracks, airfields) and specific settlements. The Research Handbook sections *Unit: Location Type*, *Unit: Location* and *Locations* describe the concept of site in more detail.

Fields

- unit:id:admin
- unit:name
- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open
- unit:site_exact_location_id_latitude
- unit:site_exact_location_name_longitude
- unit:site_country
- unit:site_feature_type
- unit:site_admin_level

- unit:site_nearest_settlement_id
- unit:site_nearest_settlement_name
- unit:site_first_admin_area_id
- unit:site_first_admin_area_name

17.3.6 Download: Personnel

Description

The “Personnel” download provides data on people holding command positions in specific units. The download is organized by the unit to which a person was posted. It contains data on the person’s posting (such as their role, rank, and title) in addition to any further biographical information (social media accounts, imagery of them, and so on). More information about how Security Force Monitor records data about persons is in the Research Handbook sections on *Persons* and *Persons Extra*.

Fields

- unit:id:admin
- unit:name
- unit:country
- unit:classification
- unit:other_names
- unit:first_cited_date
- unit:last_cited_date
- unit:first_cited_date_start
- unit:last_cited_date_open
- person:admin:id
- person:name
- person:other_names
- person:country
- person_extra:date_of_birth
- person_extra:deceased_date
- person_extra:deceased
- person_extra:account_type
- person_extra:account_id
- person_extra:external_link_description
- person_extra:media_desc
- person_extra:notes:admin
- person:posting_role
- person:posting_rank
- person:posting_title

- person:posting_first_cited_date
- person:posting_first_cited_date:year
- person:posting_first_cited_date:month
- person:posting_first_cited_date:day
- person:posting_first_cited_date_start
- person:posting_first_cited_date_start_context
- person:posting_last_cited_date
- person:posting_last_cited_date:year
- person:posting_last_cited_date:month
- person:posting_last_cited_date:day
- person:posting_last_cited_date_end
- person:posting_last_cited_date_end_context

17.3.7 Download: Sources

Description

The “Sources” download contains a list of all the sources used to evidence data on WhoWasInCommand. Unlike the other downloads, the content of the “Sources” download is not limited to a specific country: it’s everything referenced anywhere in WhoWasInCommand. To learn more about how Security Force Monitor uses sources, visit the sections of the Research Handbook about [Data integrity measures](#) and [Sources](#).

Fields

- source:id:admin
- source:title
- source:type
- source:author
- source:publication_name
- source:publication_country
- source:published_timestamp
- source:created_timestamp
- source:uploaded_timestamp
- source:url
- source:access_point_id
- source:access_point_type
- source:access_point_trigger
- source:accessed_timestamp
- source:archive_url