Ministry of Justice

HM Prison & Probation Service

Policy name: Intelligence Collection and Analysis Policy Framework

Re-Issue Date: 31 July 2025 **Implementation Date**: 18 March 2019

Replaces the following documents (e.g. PSIs, PSOs, Custodial Service Specs) which are hereby cancelled: None

Introduces amendments to the following documents (e.g. PSIs, PSOs, Custodial Service Specs):

Service Specifications altered as noted in Appendix 6.2.

Action required by:

☒	HMPPS HQ	☒	Governors
☒	Public Sector Prisons	☒	Heads of Group
☒	Contracted Prisons	☐	Contract Managers in Probation Trusts
☒	National Probation Service	☐	Community Rehabilitation Companies (CRCs)
☒	HMPPS Rehabilitation Contract Services Team	☐	HMPPS-run Immigration Removal Centres (IRCs)
☐	Other providers of Probation and Community Services	☐	Under 18 Young Offenders Institution

Mandatory Actions: All groups referenced above must adhere to the Requirements section of this Policy Framework, which contains all mandatory actions.

For Information:

Governors must ensure that any new local policies that they develop because of this Policy Framework are compliant with relevant legislation, including the Public-Sector Equality Duty (Equality Act, 2010).

How will this Policy Framework be audited or monitored: N/A

Resource Impact: None

Contact: NIU.projectspolicy@justice.gov.uk

Deputy/Group Director sign-off: Ben Farrant, Deputy Director, Security, Order and Counter terrorism, HMPPS.

Approved by OPS for publication: Michelle Jarman-Howe and Sonia Crozier, Joint Chairs, Operational Policy Sub-board.

CONTENTS

Revisions

Date	Changes
31 October 2019	A number of minor updates required throughout the document
31 July 2025	Title changed and references to intelligence sharing removed due to the publication of the Intelligence Sharing Policy Framework

1. Purpose

1.1. Purpose of Policy Framework

The policy will ensure consistent approaches to the collecting, handling, analysis and dissemination of intelligence by HMPPS. It sets out the purposes for which intelligence is collected, how it should be handled, and where/with whom that intelligence can be shared. Compliance with the policy will enable staff to have confidence that they are acting in a lawful manner, and using intelligence appropriately.

1.2. Definitions

Intelligence, for the purposes of this document, is defined as information which has been collected and analysed. Any information which has been subjected to an evaluation of the reliability of the source, the reliability of the information and the value of onward dissemination of the information, can be considered to be intelligence. Where information has been assigned an evaluation and handling code such as a 5x5x5 or 3x5x2 code, then this information should be regarded as intelligence.

1.3. Guidance for Operational staff

An accompanying restricted Intelligence Operations Manual for staff will be circulated to Establishments and Probation Local Delivery Units (LDUs) on request via NIU.projectspolicy@justice.gov.uk to provide detailed guidance on processes and tactics.

1.4. Intelligence Operations within HMPPS

HMPPS collects information for a variety of purposes, including to support offender management, for the prevention and detection of crime, preserving order and discipline in establishments, management of risk and prevention of harm, and any duty or responsibility arising from common or statute law.

Within HMPPS any information which provides an indication of the likely or actual behaviour/conduct of an offender or staff member could potentially be used as intelligence, as defined in section 1.2. It is sourced from a variety of places, and will be documented, considered and shared in a range of environments depending on the context and detail of the intelligence. Examples of intelligence can include but are not limited to:

- Observations of offender behaviour submitted by staff
- Information passed to HMPPS by another party, such as the police, victims or family members, detailing concerns about an offender's behaviour.
- Confirmed information about inappropriate/criminal activity, such as concerns that a staff member is in an inappropriate relationship with an offender.
- Anonymous information submitted by the public (e.g. Crimestoppers), such as reporting an offender in a location from which they have an exclusion area.
- Images collected by non-directed CCTV, such as video of a pass of illicit items taking place in a visits hall, or throw overs into an establishment.
- Conversations overheard by, or directly held with a HMPPS staff member (or non-directly employed staff member) where an offender volunteers information, such as a good source of drugs on a wing.
- Formal disseminations from other agencies regarding particular offenders or groups of offenders, such as a form of words indicating reasonable grounds for suspicion of criminal activity by an offender on licence, leading to consideration of recall

It is important that HMPPS staff are aware of how to appropriately collect, record, assess and act promptly on intelligence. By doing this, intelligence can be used in order to assist the prevention of crime, protect individuals and/or the organisation from harm, or promote rehabilitation, both in the community and custodial environments. For example:

- Acting on intelligence which is assessed to be reliable, prisons can combat conveyance of illicit items through targeted cell searches, or by making directed surveillance applications.
- Acting on intelligence about inappropriate behaviour/associations by an offender on licence can reduce the risk of harm through alteration of licence conditions such as increased curfews etc.

2. Outcomes

2.1. Policy Aims

2.1.1. All staff in HMPPS, Contracted Estate and CRCs understand what intelligence is and how it should be collected, handled and shared.

2.1.2. All staff are able to sanitise intelligence appropriately, protecting sources and tactics.

2.1.3. Intelligence is used correctly, where it is proportionate, necessary and justified, in order to support robust and defensible decision making.

2.1.4. Staff are confident in submitting and collecting intelligence to combat ongoing criminality in custody and community settings, to contribute to safer prisons, support robust offender management, counter security threats, and to maintain professional standards.

2.1.5. Where required, intelligence is appropriately shared within HMPPS, or disseminated to other agencies to achieve common aims and outcomes.

2.1.6. Victims, public and staff are protected as far as possible from the threat of harm through the proactive use of intelligence to identify potential risks.

2.1.7. Intelligence is recorded, handled and where appropriate destroyed in line with Data Protection requirements, on secure systems.

3. Requirements

3.1. Intelligence Collection

3.1.1. Information must be collected in order to meet the local, regional and national Intelligence Requirements. These will be set out in a range of documents including Local Tactical Assessments, Local Security Strategies, Business Plans and Strategic Assessments. Governors and LDU heads are responsible for ensuring staff are aware of these requirements.

3.1.2. National Intelligence Requirements are detailed in the executive summary of the Annual Strategic Assessment, which is circulated to the approved distribution list within HMPPS.

3.1.3. All staff are responsible for considering the types of information that may be available, and the likelihood of it having value as intelligence, based on the local and national intelligence requirements.

3.1.4. Governors must ensure that collection is managed by local collection plans. This is to ensure it remains focussed, proportionate, necessary, justified and legally compliant. However, this must not prevent staff from submitting information for a purpose that is not contained in a local or national intelligence requirement.

3.1.5. Heads of LDUs do not need to provide formal collection plans; offender managers have to collect information as referenced in section 3.1.3 under the requirements of section 198(1) (b) of the Criminal Justice Act 2003.

3.1.6. HMPPS has the ability to collect information both overtly and covertly. All covert information gathering must be authorised, in line with the Investigatory Powers Policy Framework or successor documents. This collection of information includes communications data, governed by the Investigatory Powers Act 2016, and the Investigatory Powers Policy Framework and detailed guidance (due end 2019) are to be read alongside this policy.

3.1.7. Any collection of information must be proportionate to the purpose for which it is required. Establishments and LDUs must ensure that there are processes in place to identify information which has been collected inappropriately (e.g. covertly without authority, where a handling code is missing, or precludes the sharing of that information), and to report any breaches to the originator of the information.

3.1.8. Information collected as intelligence must contain all relevant facts of what has been heard, witnessed or described, and include the details of any action taken. The reporting person should avoid including any information that does not add value.

3.2. Intelligence Analysis and Management

Governors and Heads of LDUs must ensure that:

3.2.1. Staff are aware of how to submit information for analysis in a timely manner, by the appropriate method. More information is available in the Intelligence Operations Manual.

3.2.2. All staff are aware of how to submit information which indicates a significant threat to life, risk of serious harm to persons, or threat to the order and discipline of a prison. Where the threat is in the community this must be to the relevant Law Enforcement Agency, such as Police forces, Regional Organised Crime Units, Regional Counter-Terrorism Units, National Crime Agency, UK Border Force. Where the threat is within a prison this must be brought to the attention of the duty governor via a phone call, or via internal communication methods.

3.2.3. Information, once submitted for analysis, must be stored on appropriate systems, in line with PI 2018-02 or PSI 2018-04 - Records, Information Management and Retention Policy.

3.2.4. Processes are in place to take prompt action on any intelligence 24 hours a day. This must include ensuring that appropriately trained staff have sufficient levels of access to systems to enable them to take action.

3.2.5. Intelligence received by any establishment with access to the Mercury system (e.g. HM Prisons, Contracted Estate, Secure Hospitals, Secure Training Centres) must use this system to store intelligence.

3.2.6. Intelligence received by Probation is stored on an approved case management system (e.g. National Delius), and appropriately marked to reduce the risk of disclosure to the offender.

3.2.7. All intelligence relevant to offenders with ViSOR records must also be recorded on ViSOR in line with the Mandatory Use of Visor PF Further guidance is provided in the restricted Intelligence Operations and Guidance Manual.

3.2.8. All intelligence is stored and handled in line with the handling code provided either by the intelligence originator, or by the staff member analysing the information. Where no formal intelligence grading system is in place, e.g. in probation, or a handling code is not provided, then permission to store the information and use it must be sought wherever possible from the original source of the information.

3.2.9. All intelligence, regardless of source and recording system, is considered for sanitisation, ensuring that the source of the intelligence, and the tactic used to collect the intelligence are protected. Further guidance on sanitisation is provided in the Intelligence Operations Manual in section 3.4.

3.2.10. All information is stored and managed in line with the requirements of the Data Protection Act 2018, as per Information Requests Policy Framework.

3.2.11. Intelligence is considered for destruction in a manner compliant with PSI 2018-04/ PI 02-2018 – Records, Information Management and Retention Policy. The nature of intelligence is such that retention beyond standard retention schedules in line with paragraph 5.15 of the above Instructions may be appropriate.

3.2.12. Staff working in an intelligence analysis or intelligence management role must be appropriately trained in line with the development pathway set out in the Intelligence Operations Manual. Staff may be appointed prior to training, on the understanding that failure to successfully complete such training will result in individuals being moved to alternative roles.

3.2.13. Intelligence assessments are produced and completed within the timelines set out by either the Terms of Reference for the product, within timescales set out by policy (e.g. provision of Sentence Planning and Review Form H for Parole Hearing), or as agreed by the author and requestor for ad-hoc products. The terms of reference must demonstrate the requirement for that product, i.e. that it is a proportionate and justified use of data and information.

3.2.14. Intelligence Assessments include provenance of information, ensuring that any decisions made on the basis of the assessment have robust and auditable information trails that can be provided if required at a later date.

3.2.15. Secret and Top Secret information is handled appropriately - HMPPS is able to receive and handle information and intelligence rated above Official Sensitive. Any such information should, where possible, only be received and handled by staff with the appropriate level of vetting and training, in an accredited environment. The HMPPS Sensitive Intelligence Unit (jupiter@noms.gsi.gov.uk) leads on all such intelligence receptions and handling.

3.2.16. If staff not in a secure environment are offered a briefing on material marked above Official Sensitive by a Law Enforcement Agency (LEA) then they must advise the person offering the briefing to contact the Sensitive Intelligence Unit, in order to assist the LEA and the Prison/LDU in handling the intelligence.

3.3. Additional Intelligence Management requirements for Prison Governors

3.3.1. Establishments must produce a monthly Local Tactical Assessment (LTA), identifying threat priorities, emerging and developing threats, persons of interest and concern, and intelligence gaps. A template for this assessment is available from the National Intelligence Unit, and further guidance on completion is in the Intelligence Operations Manual.

3.3.2. LTAs must be shared with the appropriate Regional Intelligence Unit on a monthly basis.

3.3.3. Prison Intelligence Units must ensure that staff only access Mercury after they have completed the required e-learning package, and preferably after having received additional work based training from an experienced member of staff.

3.3.4. Intelligence Reports on Mercury are processed in compliance with the workflow process in section 2.3 of the Intelligence Operations Manual.

3.3.5. Tasking and Co-ordination groups are held in compliance with the Tasking Framework issued by the Deputy Director of National Security Group (more detail is in the Intelligence Operations Manual).

3.4. Audit Standards – Prisons

3.4.1. Prison Governors must ensure that Security and Intelligence Units are operating in Compliance with the relevant audit baselines. These are available via the HMPPS intranet.

4. Constraints

4.1. Intelligence Evaluation and Handling Codes

HMPPS is clear that these codes are not Personal Data as defined by the Data Protection Act 2018. Therefore an offender, or person acting on behalf of an offender, requesting his or her personal data has no right of access to the codes that relate to an intelligence report, even if that intelligence report does contain his or her personal data.

4.2. Intelligence Management systems, e.g. Mercury

Required free text fields such as the intelligence assessment field in Mercury must contain meaningful content, e.g. not cut and pasted from previous fields, or single characters such as “x” or “.”. Where the staff member entering information is not able to provide that meaningful content as it is outside of the scope of their role then the following wording must be used; “Submitted for analysis”. Further detail can be found in the Intelligence Operations Manual in section 3.4.

5. Guidance

5.1. Analytical Language

It is important that Intelligence Assessments use common language and approaches to describing findings, to allow accurate and useful comparison of judgements. The ‘Yardstick’ is a tool which assists the selection of verbal probability terms to illustrate the likelihood of events or developments described in the intelligence product. The probability and analytical confidence statements articulate the uncertainty surrounding an intelligence judgement.

The Government Professional Head of Intelligence Analysis (PHIA) based in Cabinet Office, design and control the clearly defined analytical and predictive language Intelligence analysts use in their reporting. The language conforms to standard reporting language used throughout HM Government and aids cross department standardisation and collaborative working. It is suggested that it is presented as an annex within analytical products and is known as the probability yardstick, which was last updated March 2018.

The use of consistent and clearly defined analytical language has two main values. Firstly it encourages the analyst to think about how they are presenting their assessments and forces them to quantify the likelihood of their assessments. Secondly the reader is clear on the analyst assessment and can easily compare assessments made from different government sources.

For example, a Minister reading analytical intelligence products produced by HMPPS, Defence Intelligence and JTAC will have a better understanding of the overall risk and threat because all the analysts are using the same range of probability when discussing likelihood. The probability ranges below act as guidelines for the language used to describe likelihood. The intentional gaps between the ranges are to encourage intelligence analysts to be clear about what their assessments mean. Given the inherent uncertainty when assessing intelligence, this precludes debating whether something is at the lower end of one range or the upper end of the one below it.

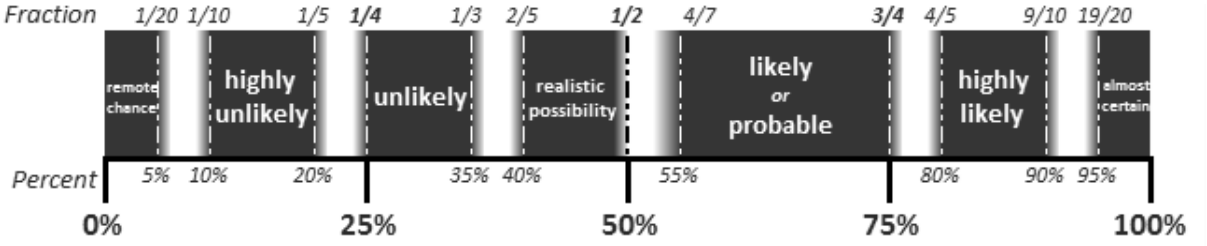

Figure 1 The Probability Yardstick

5.2. Intelligence Grading

The grading of intelligence reporting provides a shared understanding between law enforcement communities and partner agencies of the reliability of intelligence. Reporting used in this product is informed by the 5x5x5 evaluation process allowing analysts to communicate a confidence in the reporting through use of agreed analytical and predictive language. Some agencies have now adopted a 3x5x2 process for grading intelligence, the table below shows a comparison between the two formats.

Source Evaluation	(A) Always Reliable	(B) Mostly Reliable	(C) Sometimes Reliable	(D) Unreliable	(E) Untested Source
	Reliable		Not Reliable		Untested
Information & Intelligence Evaluation	(1) Known to be true without reservation	(2) Known personally to the source but not to the officer	(3) Not known personally to source but corroborated	(4) Cannot be judged	(5) Suspected to be false
	(A) Known directly	(B) Known indirectly but corroborated	(C) Known indirectly	(D) Not known	(E) Suspected to be false
Handling codes	(1) Within UK police service and other law enforcement agencies as specified	(2) To UK non-prosecuting parties	(3) To non-EU foreign law enforcement agencies	(4) Within originating agency/ service	(5) Receiving agency to observe conditions as specified
	P – Lawful sharing permitted.			C – Lawful sharing permitted with conditions.	

5.3. What Makes a Good Intelligence Report?

When submitting an IR, staff should consider the requirements against which they are submitting the IR, and ensure that it has value for the person analysing the report for further action. The factors that go into making a good IR are summarised in the picture below. Not all of the items below will be possible to include in every IR, but as many as possible should be present.

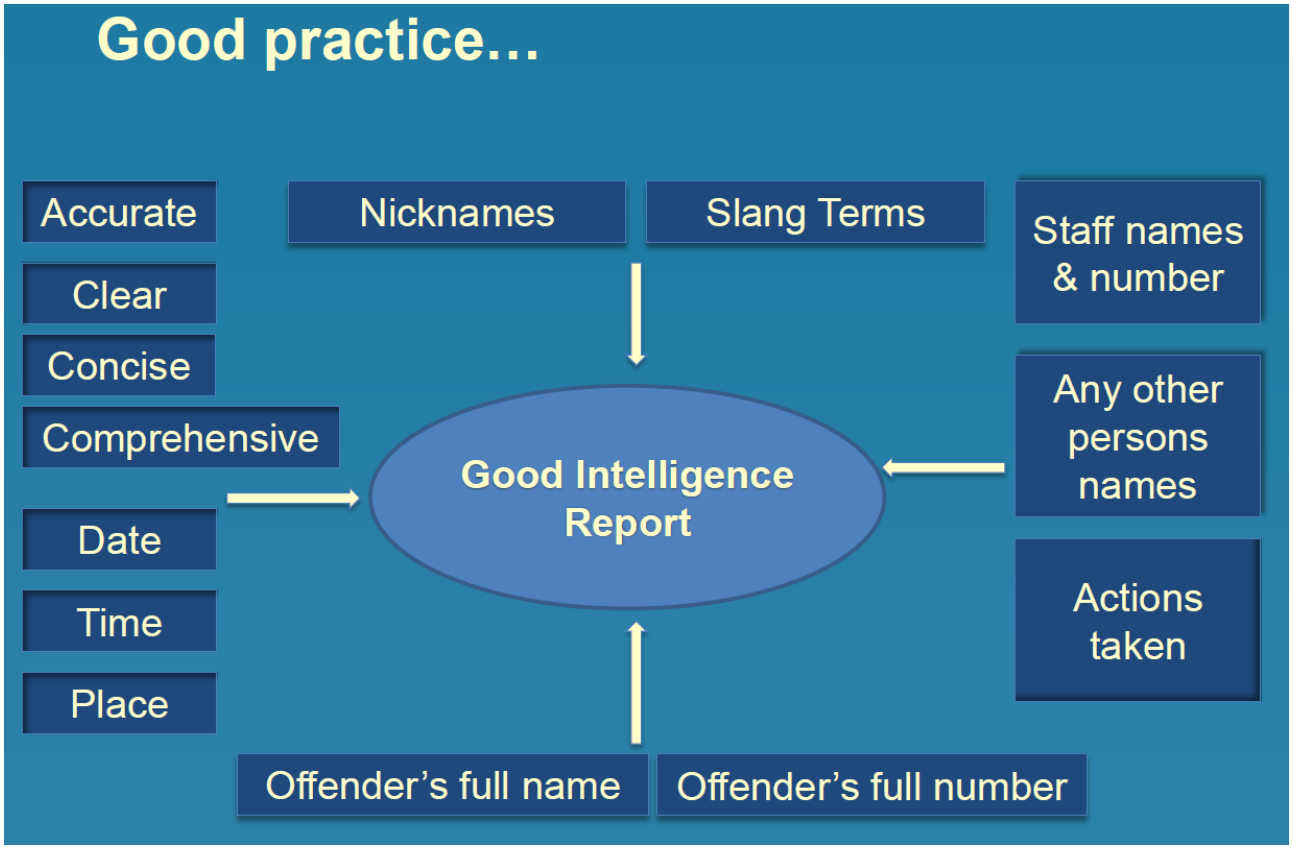

Figure 2 - What makes a good IR?

5.4. Sanitisation and Redaction – Definitions

Redaction and Sanitisation are two different processes, used for different purposes. It is important that the officer preparing a document or intelligence for dissemination is clear on the difference, and which process is appropriate.

Sanitisation is normally achieved by producing a form of words structured to obfuscate the origin and not merely replacing details of the source or tactic with 'XXXX'. The wording should not identify the source or capability explicitly or implicitly. Care should be taken to ensure that if reporting is derived from the same source, amalgamation of all the intelligence reporting does not, inadvertently, disclose the nature of the source or identity. As a general principle, all intelligence should be considered for the application of sanitisation, in order to prepare it for dissemination at the earliest opportunity.

Redaction is "the separation of disclosable from non-disclosable information by blocking out individual words, sentences or paragraphs or the removal of whole pages or sections prior to the release of the document. This should be done on a paper copy and then scanned, or using specific redaction software in line with the guidance produced by the Information Commissioner's Officer." (Redaction Toolkit, National Archives)

More guidance on redaction is provided by the National Archives, and the Information Commissioner's Office

Appendix

6.1 Service Specifications impacted by this Policy

The table identifies specifications which are impacted by this Policy Framework (PF) in the following ways:

- **Mandatory Instruction** – The PF includes instructions which, if not followed, would prevent delivery of the specification
- **Supports** – The PF provides instruction/details which when implemented will enable the delivery of the specification
- **Replaces –** The PF includes instructions which supersede the specification due to new products/processes or systems

Service Specification	**Section(s)**	**Impact** (relevant sections of policy hyperlinked)
Security Management	References for Detailed Mandatory Instructions and all specifications affected: 16 – 34,	This Policy Framework replaces the following as the relevant mandatory instruction: NSF 4.1: PSI xx/xxxx Intelligence, NSF 4.2: PSI xx/xxxx Sharing Intelligence NSF 4.3: PSI xx/xxxx The Mercury Intelligence System (MIS)
	16	**Mandatory Instruction** Policy introduces requirement for staff involved in intelligence development and management to achieve relevant training standards (3.2.4 and 3.2.16)
	17	**Mandatory Instruction** Policy introduces requirement to produce Local Tactical Assessment to support delivery of specification (3.3.1)
	19	**Replaces** Policy mandates the use of Mercury for recording of information that may be developed as intelligence (3.2.5)
	22 - 23	**Supports** Policy requires use of Intelligence Requirements, and collection plans against identified threats, including escape risk (3.1)
	33	**Supports** Policy includes new Information Sharing Agreement for exchange of intelligence with bordering jurisdictions (3.4.7)
	44	**Mandatory Instruction** Policy Framework to be regarded as Mandatory Instruction. In particular the use of Local Tactical Assessments to inform collection plans and intelligence development. (3.3.1)
Cell and Area Searching	References for Detailed Mandatory Instructions	Policy Framework to be regarded as mandatory instruction in delivery of specification
	4	**Supports**

Service Specification	Section(s)	**Impact** (relevant sections of policy hyperlinked)
		Outputs of Policy including Local Tactical Assessment to be used in supporting the assessment of risk for cell and area searches
	9 & 10	**Mandatory Instruction** Policy and associated manual introduce multiple instructions for development of intelligence, including but not limited to: • Assessments of local intelligence picture (3.3.1) • Training requirements (3.2.4 and 3.2.16) • Use of Mercury (3.2.5) • Dissemination of intelligence internally (6.1).
Prisoner Discipline and Segregation – Segregation of Prisoners	3	**Supports** Policy directs the appropriate dissemination of intelligence, and the format for communicating this to prisoners where used to inform decision making (6.1). Guidance also provided in restricted manual
	5	**Supports** Policy directs the use of intelligence to identify risk levels and decision making around issues including segregation (3.4.7, 6.1)
Nights	1	**Mandatory Instruction** Policy introduces requirement for sufficient staff trained in use of Mercury to be available at all times to process Intelligence reports in a timely manner (3.2.4)
Prisoner Communication Services	Mandatory Detailed Instructions and Specifications 10 - 14	NSF Function 4 to include this Policy Framework

The following Service Specifications contain references to intelligence or activity where intelligence will support activity, and therefore consideration of this Policy Framework should improve the delivery of these specifications:

Title	**Specifications** (NB - others may also be relevant)
Early Days & Discharge – Reception in	8
Provision of Secure Operating Environment: Communication & Control Rooms	6 & 7
Provision of Secure Operating Environment: Gate Services	7
Activity Allocation	3 & 8
Manage the Custodial and Post Release Periods	33, 42 and 57
Manage the Sentence for a Community Order or Suspended Sentence Order	18 - 19