Department of
Finance
An Roinn
Airgeadais
www.finance-ni.gov.uk

Mr Jim McManus
Finance Committee Clerk
Northern Ireland Assembly
Parliament Buildings
Stormont
Belfast
BT4 3XX

Private Office
2nd Floor
Clare House
303 Airport Road West
BELFAST, BT3 9ED
Tel: 028 9081 6216
Email: private.office@finance-ni.gov.uk

Your reference:
Our reference: SUB 1202 2020

Date: 13th June 2020

Dear Jim,

FUNCTIONING OF GOVERNMENT (MISCELLANEOUS PROVISIONS) BILL: COMMITTEE STAGE

Thank you for your email of 14 May, attaching additional questions from the Committee in respect of the Department's previous written response. I attach responses to the questions.

There are a number of points on which the Department would provide a general response.

As the Minister set out in his evidence to the Committee, it is the view of Ministers that the issues contained in the Bill have been addressed in the revised Codes and Guidance, and that it is not necessary to bring forward legislation. There is, therefore, no question of whether the Department will accept any of the clauses if the drafting issues are addressed; the Department's position is that it does not accept any of the clauses.

If the Executive believes that the recommendations of the RHI Inquiry call for further amendment of the Codes and Guidance, this will be taken forward through the Executive Subcommittee, chaired by the Minister of Finance. That Subcommittee has not yet met, as a result of the exceptional situation in which government is currently operating, but the Executive has set out its commitment to the Subcommittee in the *New Decade, New Approach* Agreement. It is worth noting that such changes will be much more easily effected through the revision of Codes than through the amendment of provisions contained in primary legislation.

On the matter of drafting, while the Department has concerns about the unintended consequences of some of the drafting, it is not for the Department to resolve those issues; that is a matter for the Member bringing the Bill. Moreover, it would be for the Member to satisfy the Committee that any such flaws have been addressed before the Bill progresses.

The questions around clauses 6, 7 and 8 ask whether the Codes and Guidance sufficiently respond to the issues that gave rise to the Bill's provisions. The Department is aware of the findings and conclusions of the RHI Inquiry, and Ministers have committed to review the existing Codes and Guidance in light of the Inquiry's recommendations, through the Executive Subcommittee on Reform following the RHI Inquiry.

I also attach a copy of the NICS *Guide to Physical, Document and IT Security*, which is relevant to the Committee's consideration of clause 9. Apologies that this was not provided earlier.

Yours sincerely,

Ciara McKay

CIARA McKAY
DEPARTMENTAL ASSEMBLY LIAISON OFFICER

ENC.

Functioning of Government (Miscellaneous Provisions) Bill

Questions for Response to the Committee for Finance

The following questions mostly relate to the written evidence provided by the Department of Finance in response to a call for evidence to the Department, the Head of the Civil Service and Permanent Secretaries. As a single response was provided in response to the call for evidence, a similar approach has been adopted in seeking further evidence on behalf of the Committee for Finance. Other Assembly committees may wish to ask additional questions.

Clause 1(2)

1. The response states that only FM and dFM SPADs can form groups with an internal hierarchy. What is currently in place to prevent parties acting informally outside of this structure?

   In terms of their role within government, individual SpAds are accountable to the Minister who appointed them. Within the offices of the First Minister and deputy First Minister it would be possible for the Ministers to delegate aspects of their management role in respect of their special advisers to one special adviser, thus creating an internal hierarchy. In other Ministers' offices, there is only one special adviser, so there is no capacity for the Minister to delegate his or her management responsibility to anyone else.

   There are no impediments to individual special advisers working within informal groups and networks, and this is provided for in the *Code of Conduct for Special Advisers* (paragraph 4).

Clause 1(3)

2. The response states that the revised Special Adviser and Ministerial Codes of Conduct make clear that Ministers are responsible and accountable for the conduct and discipline of their special advisers.

   a. What sanctions are in place to deal with misconduct?

      Ministers are responsible for the conduct and discipline of their special advisers, including their adherence to their *Code of Conduct*. Depending on the nature of the breach, a range of sanctions is available to Ministers, up to and including dismissal.

   b. Who determines when there has been misconduct?

Whilst the investigation of misconduct may, for instance, be undertaken by a civil servant, the Minister is ultimately responsible for the discipline of a special adviser, though the civil service may be expected to contribute and their advice may be made public.

c. Who determines what sanctions should be imposed once it has been determined that misconduct has occurred?

As above.

d. To what extent are ministers satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases?

All Ministers have agreed the current codes and guidance. There will be a key role for the NICS, acting impartially and objectively.

3. The response states that, as temporary civil servants, NICS disciplinary processes may be applied to special advisers, but may need to be modified to take account of the special status of special advisers. In particular, the disciplinary processes assume a civil service line manager and a chain of line management, which special advisers will not have. The response refers to drafting problems relating to the involvement of a minister in the disciplinary process.

a. Is this a suggestion that the NICS disciplinary process will, or should be amended to include modifications appropriate to SPADs?

No. The Handbook must be interpreted to take account of the different status of special advisers.

b. If the drafting issues can be resolved, is the Department content to accept this provision subject to appropriate modifications to the NICS disciplinary processes?

No. This provision is unnecessary.

c. Please make suggestions for addressing the drafting issues referred to.

The drafting of the Bill is a matter for the member.

d. Would it be appropriate or acceptable for a process to remain in place where a Minister could ignore sanctions recommended by officials resulting in no action being taken against a special adviser who has been found to have contravened the Code of Conduct?

No. There will be a key role for the NICS in this process. If a Minister chooses not to apply the disciplinary process or act upon the conclusions of that process, he or she may be challenged in respect of their responsibility for the conduct and discipline of their special adviser. The decision of the Minister and the civil service advice may be made public. Any failure to fulfil that responsibility may be referred to the Ministerial Standards Panel. A breach of the Ministerial Code of Conduct may be considered a breach of the Pledge of Office and therefore subject to the existing sanctions by the Assembly.

Clause 1(4)

4. The response states that an appointment that does not meet the provisions of the Code for Appointment would not be lawful.

    a. Can the Department outline the specific provisions of the Code of Appointment relating to this and how this meets the provisions of Clause 1(4)?

    Section 8(2) of the Civil Service (Special Advisers) Act (NI) 2013 sets out that where a Minister proposes to appoint a special adviser, such an appointment shall be subject to the terms of the code. An appointment that is not subject to the terms of the Code would therefore be unlawful.

    b. Should it later be determined that a SPAD has been appointed outside of compliance with the Code of Appointment, what would happen?

    The appointment would be withdrawn and salary recovered.

Clause 1(5)

5. The response states that the new arrangements for special adviser pay set a maximum of £85,000. The Grade 5 maximum is currently £80,847. No special adviser is currently paid more than the Grade 5 maximum and that legislation is not, therefore, required.

    a. Please confirm that, because no SPAD is currently paid more than the Grade 5 maximum, this does not prevent a future situation where a SPAD may be paid up to more than £4,000 more.

    Decisions on special adviser pay are made in line with the policy 'Remuneration of Special Advisers' which sets a maximum of £85k.

    The policy is set out at:

https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/REMUNERATION%20OF%20SPECIAL%20ADVISERS%20-%20FINAL%20-%2020%20JANUARY%202020.pdf

There are no plans to increase the payband.

b. Please outline in detail the objections to aligning SPAD pay to NICS pay scales.

Special advisers have a distinct role within the NICS, and like other distinct groups within the NICS, they have a separate pay scale. Special advisers in other UK jurisdictions also have a separate pay scale.

c. Given that SPAD pay levels now range from around Grade 7 to Grade 5, would the Minister be amenable to introducing a grading system for SPADs based on a job evaluation with pay levels at NICS Grade 7 to Grade 5?

Comparison with the kinds of work done at Grade 7 and Grade 5 was one of the key factors in the setting of the existing special-adviser pay scales. The pay scales are not precisely the same as those for general-service civil servants, not least to avoid the conclusion being reached that the role of special adviser is the same as that of a general-service civil servant at a similar grade.

d. Is DOF aware of what arrangements are in place in other jurisdictions for payment of SPADs and what consideration was given to this in deciding the pay levels for SPADs in Northern Ireland?

The pay for special advisers in the other UK jurisdictions is published on a regular basis and this information was taken into account by DoF. The latest published information is to be found at

- https://www.gov.uk/government/publications/special-adviser-data-releases-numbers-and-costs-december-2019
- https://gov.wales/written-statement-special-advisers-3
- https://www.parliament.scot/parliamentarybusiness/28877.aspx?SearchType=Advance&ReferenceNumbers=S5W-26805&ResultsPerPage=10
- https://assets.gov.ie/19699/67fe34e66f084372b5f17066e8c8bb75.pdf

e. Is it the case that the pay for SPADs in Northern Ireland is generally higher than in other devolved administrations and, if so, can DOF outline the justification for this?

No, this is not the case. Pay for Special Advisers in NI is broadly in line with that in UK devolved administrations.

Clause 1(6)

6. The response states that the Code of Conduct and contract of employment already includes provision for only a properly constituted SPAD being able to fulfil the functions of a SPAD and, that anything else would be unlawful.

a. Please outline where in the Code of Conduct and the contract of employment these provisions exist.

The earlier response from the Department stated that the position is already *inherent* in the Code of Conduct and contract of employment; anything else would be unlawful. The Code of Conduct and the Letter of Appointment set out the role and responsibilities of a special adviser, that is, a person appointed to a position in the NICS under article 3(2)(b) of the Civil Service Commissioners (NI) Order 1999; they do not apply to anyone else.

b. If it is the case that the provisions are already included, how did this not prevent a situation in the past where a person who was not a SPAD could act as a SPAD?

The revised *Ministerial Code of Conduct* has been strengthened and now places explicit requirements upon Ministers (a) to ensure that official resources are not used for party political purposes and (b) to comply with the rules regarding the management of official information.

c. Is the Minister in agreement with the broad principles that this provision seeks to make and, if so, would the Minister be open to a suitably drafted amendment to address the issues identified in the response?

The Minister's view remains that the provision is unnecessary.

d. Please make suggestions for addressing the drafting issues referred to.

The drafting is a matter for the Member.

Clause 2

7. The response states that reducing the number of SPADS for FM & dFM to one each does not recognise the seniority or weight of the role.

    a. Please outline in detail the seniority and weight of the roles of SPADs in The Executive Office including the internal structure.

    There are three Special Advisers appointed each by the First Minister and deputy First Minister. These have a wider range of responsibilities than those appointed by other Ministers. These responsibilities include: supporting the First Minister and deputy First Minister in the discharge of their joint responsibilities and in joint decision making; advising and supporting the First Minister and deputy First Minister in relation to the functions of the Executive Office; consultation with other special advisers in support of collective decision making by the Executive Committee and of the role of the First Minister and deputy First Minister as joint chairs.

    b. If reducing to one each is considered too few, what would be considered an appropriate level to reduce the number to and still recognise the seniority and weight of the role?

    This would be a matter for the First Minister and deputy First Minister to determine jointly.

    c. Please outline the role of each of the SPADs in TEO and explain why the currently employed number of SPADs is appropriate?

    The role of special advisers in TEO is described above.

8. It is recognised there are currently six SPADs in TEO, however, there has previously been eight SPADs employed in TEO.

    a. Is it considered appropriate that there should be provision for eight SPADs in TEO and, if so, how can this be justified?

    The earlier response refers. The statutory complement of eight special advisers has not been filled during this mandate.

    b. Is DOF aware of the arrangements in other jurisdictions for determining the number of SPADs?

    Para 3.2 of the UK Government's Ministerial Code says "With the exception of the Prime Minister, Cabinet Ministers may each appoint up to two special advisers. The Prime Minister may also authorise the appointment of special advisers for Ministers who regularly attend Cabinet. All appointments, including exceptions to this rule, require the prior written approval of the Prime Minister".

There are no similar rules determining the number of special advisers in other devolved UK jurisdictions.

c. Outline in detail why the number of SPADS in Northern Ireland varies so much from that of other devolved administrations?

This is not the case.

The number of special advisers broadly reflects the spread of governmental responsibilities in each of the devolved jurisdictions:

- Scotland has a First Minister, eleven Cabinet Secretaries and 14 special advisers;
- Wales has a First Minister, eight Ministers and 14 special advisers (12 full-time equivalent);
- Northern Ireland has a First Minister and deputy First Minister, eight Ministers and 13 special advisers.

By comparison, the UK Government comprises 119 Ministers and 108 special advisers.

The latest published information for the other jurisdictions is available at the links set out at paragraph 5(d) above.

Clause 3

9. The response states that no appointments have been made under this provision by this administration and that the provision is being kept under review.

a. Do relevant ministers believe that this response adequately addresses any issues that there may be within TEO/DOF in relation to this Clause?

Clause 3 subjects the prerogative power of the FM and dFM in relation to the NICS and the Commissioner for Public Appointments for Northern Ireland under section 23(3) of the Northern Ireland Act 1998 in its entirety to Assembly approval and therefore constitutionally represents a significant change to the traditional authority of the executive arm of government in the management of the civil service.

The clause also repeals the Civil Service Commissioners (Amendment) Order (Northern Ireland) 2016 which was made under section 23(3) and which allowed the FM and dFM to appoint a person to provide specialised support outside the requirement for selection on merit on the basis of fair and open competition.

The effect of the provision would therefore be to prevent the First Minister and deputy First Minister engaging specialised expert support in an emergency situation where the normal procedures for appointments may be insufficiently responsive to the urgency of the matter.

b. The response does not raise any objection to this Clause, can the Committee, therefore, conclude that Clause 3 is supported?

No. As set out in the covering letter, the Department's position is that it is not necessary or appropriate to legislate in this area, therefore no clause is supported.

c. Is it recognised that, although no appointments have been made by this administration, the facility exists in legislation for this to happen and, therefore, the only way to prevent this from occurring in the future is through legislation?

Yes.

d. In relation to the provision being kept under review:

i. What is meant by this and how is this being done?

The power to appoint will be considered in the context of ongoing civil service reform.

ii. Please demonstrate to the Committee any evidence that there has been a decision to keep this under review or that it has been reviewed in any way.

The provision was considered at the time of the review of the codes of Conduct and will be kept under review.

The appointment of expertise to the NICS is a matter of ongoing consideration.

Clause 6

10. The response states that the requirement upon civil servants to keep accurate official records, including minutes of ministerial meetings, is contained in the revised NICS Code of Ethics. It further states that the Code does not set out the degree of detailed contained in this clause which, the response states, appears to be unnecessarily specific.

a. Please outline how the Code of Ethics address the issues that gave rise to this provision.

The inclusion for the first time of this requirement at paragraph 8 of the Code of Ethics places a duty upon all civil servants to keep accurate official records.

b. Please outline in more detail why this clause is considered unnecessarily specific.

A minute should be proportionate and useful. It would be contrary to good information management for every minute of every discussion to be as comprehensive as this clause would require.

c. Please demonstrate how the current provisions are sufficiently robust under all circumstances to prevent ministers meeting with civil servants without an official record of such a meeting being made.

The inclusion of reference to record-keeping within the *NICS Code of Ethics* and the *Ministerial Code of Conduct* requires the keeping of accurate records.

d. What level of specificity would be appropriate?

It is not appropriate to legislate in this area.

Clause 7

11. The response states that the Guidance for Ministers sets out ministers must ensure that records of meetings are maintained. It also states that the NICS Code of Ethics includes the requirement upon civil servants to keep minutes of ministerial meetings.

a. Please outline how the Code of Ethics address the issues that gave rise to this provision.

The inclusion for the first time of this requirement at paragraph 8 of the Code of Ethics places a duty upon all civil servants to keep accurate official records.

b. To what extent can there be certainty that the Code of Ethics will result in accurate minutes being kept of all meetings in all circumstances?

The *Code of Ethics* is a part of civil servants' terms and conditions of service. Breaches of the Code constitute a breach of contract and can lead to disciplinary measures, up to and including dismissal.

It is also a requirement that Ministers' private offices are responsible for taking such notes, whereas previously it was a duty placed upon the policy officials. The requirement to keep good records is included in the Private Office guidance.

c. Please demonstrate how the current provisions are sufficiently robust under all circumstances to prevent ministers and special advisers from failing to record all meetings with non-departmental personnel about departmental matters?

Ministers are bound by the *Ministerial Code of Conduct* to adhere to the rules regarding the management of official information. These rules are expanded upon in section 7 of the *Guidance for Ministers*, and include the requirement to ensure that an appropriate official attends all meetings concerning departmental or Executive business, and that records of all such meetings are maintained. The *Guidance* also sets out what to do if it is not possible for an official to be in attendance.

The consequences for a Minister of failing to fulfil these requirements arise from his or her breach of the *Ministerial Code of Conduct* and therefore of the Pledge of Office.

Special Advisers are bound by the *NICS Code of Ethics* and subject to the same consequences of any breach of that Code.

Clause 8

12. The response states that the NICS Code of Ethics requires civil servants to keep accurate minutes of ministerial meetings. The response also raises some drafting issues.

a. Please outline how the Code of Ethics address the issues that gave rise to this provision.

The Code of Ethics requires civil servants to keep accurate official records, including minutes of ministerial meetings.

b. To what extent can there be certainty that the Code of Ethics will result in accurate minutes being kept of all meetings in all circumstances?

The Code of Ethics is a part of civil servants' terms and conditions of service. Breaches of the Code constitute a breach of contract and can lead to disciplinary measures, up to and including dismissal.

As set out in the Department's initial response, the terms of the *Ministerial Code of Conduct* and the *Guidance for Ministers* also work to

ensure that accurate minutes are kept of all meetings in all circumstances.

c. Please demonstrate how the current provisions are sufficiently robust under all circumstances to prevent ministers and special advisers from failing to record all meetings with non-departmental personnel about departmental matters.

Ministers are bound by the *Ministerial Code of Conduct* to adhere to the rules regarding the management of official information. These rules are expanded upon in section 7 of the *Guidance for Ministers*, and include the requirement to ensure that an appropriate official attends all meetings concerning departmental or Executive business, and that records of all such meetings are maintained. The *Guidance* also sets out what to do if it is not possible for an official to be in attendance; if a Minister meets an external organisation or individual and finds themselves discussing official business without an official present any significant content should be passed back to their Private Secretary as soon as possible after the event.

A Minister failing to fulfil these requirements may be referred to the Ministerial Standards Panel.

Special Advisers are bound by the *NICS Code of Ethics* and subject to the same consequences of any breach of that Code.

d. Please make suggestions for addressing the drafting issues referred to.

The improvement of the drafting is a matter for the Member.

Clause 9

13. The response does not address the provisions relating to the use of non-official electronic systems. Please provide detailed views in relation to this provision to assist Committee scrutiny of the Clause.

The response to the Committee set out the existing requirements upon Ministers and civil servants, including special advisers, in respect of the use of non-official electronic communications systems.

The Guidance for Ministers states:
Ministers must use official email systems for all communications relating to official business. Exceptionally, where this is not possible, the Minister must copy any message to their official email account. Information generated in the course of government

The Code of Conduct for Special Advisers states:
Special Advisers must use official email systems for communications relating to official business. Exceptionally, where this is not possible, the Special Adviser must copy any message to their official email account. Information generated in the course of government business must be handled in accordance with the requirements of the law (including the Freedom of Information Act (FoI), GDPR and Public Records Act), regardless of how it is communicated.

The NICS has a *Use of Electronic Communication* policy which recommends that private email addresses are not used for business purposes and highlights that information held in non-work personal email accounts may be subject to the FOI.

As set out in the covering letter, the Department's position is that it is not necessary or appropriate to legislate in this area, since there already exists sufficient provision in Codes and guidance.

In addition, we would refer to the *Guide to Physical, Document and IT Security* (a copy is attached), which sets out the requirements for proper handling of official information. This document is currently under review. The Department apologises for failing to provide this document in the first instance.

14. The response also refers to the Code of Conduct for SPADs stating that they must use official email systems for communications and, where this is not possible, they must copy any message to their official email account.

    a. What checks and balances are in place to ensure that this happens?

    Civil Servants, including departmental Private Offices, will respond to any concerns that private email accounts are being used. The Minister is responsible for the special adviser's compliance with the *Code of Conduct*.

    b. What sanctions are in place where it is found that this has not happened?

    Breach of the *Code of Conduct* can lead to disciplinary action being taken.

    c. To what extent is the Minister of Finance satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases?

    The Minister is satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases.

15. The response refers to the Use of Electronic Communication policy which *recommends* that private email addresses are not used for business purposes.

    a. Does this policy apply to ministers and SPADs?

    The *Use of Electronic Communications* policy forms part of the NICS Handbook, and as such applies to special advisers.

    The *Guide to Physical, Document and IT Security* has general application.

    b. Is it appropriate that this is only a recommendation?

    The *Use of Electronic Communication* policy and the *Code of Conduct for Special Advisers* recognise that there are times when it may, exceptionally, be appropriate or necessary for an official to use a private email account to communicate on official business.

    c. What checks and balances are in place to ensure that this policy is complied with?

    Any use of private email accounts that is uncovered would be brought to the attention of the individual's line manager (in the case of a special adviser, to the Minister and the Permanent Secretary), and would be addressed in line with the existing discipline policy.

    d. What sanctions are there in place where the policy is not complied with?

    Breach of the policy can lead to disciplinary action being taken, and the Committee has been provided with evidence of instances of dismissal for such breaches.

    e. To what extent is the Minister of Finance satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases?

    The Minister is satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases.

16. The response states that the creation of criminal offences does not form part of the current policy. This statement seems somewhat unnecessary because, as with other clauses in the Bill, if it did form part of current policy, there would be no requirement for a clause to introduce such a provision. Why was this statement included?

    This statement was included to underline the position of the Minister, as set out in the covering letter, that he opposes this Bill.

17. The response raises some issues with the drafting of the Clause.

    a. If the drafting issues can be resolved, will this provision be accepted?

       No. This provision is unnecessary.

    b. Please make suggestions for addressing the drafting issues referred to?

       The drafting of the Bill is a matter for the Member.

Clause 10

18. The response refers to the Ministerial Declaration of Interest Framework to be completed by ministers upon assuming office.

    a. Please demonstrate that this fully complies with the provision to require the creation and publication of a register of interests for ministers.

       There is no substantive difference between the requirements within the Bill and the existing requirements upon Ministers, brought in for the first time in January 2020.

19. In relation to declarations of interests:

    a. Are the proposed timeframes provided for publication feasible/practical or would alternative timeframes need to be considered?

       The timeframes do not appear to be unreasonable.

    b. The response does not state that ministers' relevant interests will be published. Why not?

       The response from the Department quotes the *Guidance for Ministers* as saying 'a statement covering relevant Ministers' interests will be published twice yearly.'

    c. When will SPADs' interests be published?

       Arrangements are being made to publish special advisers' relevant interests shortly.

20. The response refers to the Code of Conduct for SPADs.

    a. Please demonstrate that this fully complies with the provision to require the creation and publication of a register of interests for SPADs?

There is no substantive difference between the requirements within the Bill and the existing requirements upon Special Advisers.

Clause 11

21. The response refers to the Code of Conduct for SPADs. It states that special advisers *should* not disclose official information.

    a. To what extent can this be considered a robust prevention measure when it states merely that special advisers *should* not disclose official information?

    Unauthorised disclosure of official information is a disciplinary matter, and, depending upon the seriousness of the case can lead to dismissal and/or criminal proceedings.

    b. What checks and balances are in place to ensure that this is complied with?

    Any unauthorised disclosure that is uncovered will be investigated, and if a special adviser is found to be responsible it will be brought to the attention of the Minister, who is responsible for the discipline of the special adviser.

    c. What sanctions are there in place where the policy is not complied with?

    A range of sanctions is available, up to and including dismissal.

22. The response refers to some drafting issues including the potential to criminalise the communication of any official information.

    a. Please outline in what way the Clause, as drafted, may cause the communication of any official information to be criminal as claimed.

    The Bill contains no definition of 'confidential', and that term may be interpreted widely to include any material that is not published or intended for publication. The clause is broadly drafted, and it could lead to the situation where only published material could be communicated with anyone else, even within government, about anything which might be of benefit to anyone else, which would include most public-sector activity.

It is also important to note that the draft clause also makes no allowance for departments to communicate commercially sensitive information with contractors, as appropriate.

b. To what extent is the Minister satisfied that the current sanctions would be applied, fairly, openly and consistently in all cases?

The Minister is satisfied that the policy is appropriately applied at present.

c. If the drafting issues can be resolved, will this provision be accepted?

No. The provision is unnecessary.

d. Please make suggestions for addressing the drafting issues referred to?

The drafting of the Bill is a matter for the member.

23. The response states that it is not clear how this provision is meant to interact with the Freedom of Information Act. Please outline the Freedom of Information implications of this Clause.

The Freedom of Information Act enables a member of the public to request information currently held by public bodies. As above, without a definition, any material that is not already published or intended for publication might be considered confidential. It would, therefore, be a criminal act under *this* provision for the Department to disclose information that the FOIA requires to be disclosed.

Additional

24. During the oral evidence session, the Permanent Secretary mentioned that the Private Secretary role had been upgraded two grades from Staff Officer to Grade 7. The NICS operates a robust system of Job Evaluation and Grading Support (JEGS) to ensure that the grades of all administrative roles in the NICS are commensurate with job weight. Can the Department confirm if, and when, a JEGS evaluation was completed for the Private Secretary role prior to the role being upgraded?

In February 2019, the NICSHR Grading Unit was asked to provide an independent view on the appropriate grade of the proposed revised Private Secretary role. The JEGS evaluation was applied and it was determined that the proposed role should be graded at Grade 7.

Northern Ireland Civil Service

A Guide to Physical, Document and IT Security

Incorporating the New Government Security Classifications

This document replaces the Guide to Document and IT Security issued August 2010
Effective date: 2 April 2014

Contents

1. Aims of this Guide

Protective security measures are in place for the protection of staff and the safeguarding of official information, material and assets. Protective security measures cover physical (buildings/estates/ property), personnel (staff/contractors/ customers) and information (documents/data systems) security.

This Guide is intended to provide a ready reference on matters relating to physical, document and IT security. The standards and procedures in the guide are the basic minimum which must be applied uniformly throughout all NICS Departments* and Agencies. It applies to all information collected, stored, processed, generated or shared to deliver services and conduct business, including information received from or exchanged with external partners.

Security of Information

NICS information assets may be classified into three types: **OFFICIAL**, **SECRET** and **TOP SECRET**. Each attracts a baseline set of security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated data or to manage integrity and availability concerns. The vast majority of NICS information will be classified as **OFFICIAL**.

Everyone who works with or within government has a duty to respect the confidentiality, availability and integrity of any NICS information and data that they access, and is personally accountable for safeguarding information in line with this policy. The NICS rely on you, with guidance from your managers and departmental policy, to make sure it is protected appropriately. **ALL** government information must be handled with care to prevent loss or inappropriate access, and deter deliberate compromise or opportunist attack. You are personally responsible for securely handling any information that is entrusted to you in line with local business processes (e.g. physical storage or use of TRIM access controls). You should not divulge any information gained as a result of your work to any unauthorised person and you may be liable to disciplinary or criminal procedures if you do so.

NICS Departments and Agencies should apply the principles set out in this Guide and ensure that consistent controls are implemented throughout their public sector delivery partners (i.e. Non-Departmental Public Bodies (NDPB's) and Arms Length Bodies (ALB's)) and wider supply chain.

*Department of Justice staff should also refer to DoJ policies and standards when handling information above **OFFICIAL**.

2. Government Security Classifications

Overview

The Government Security Classifications is an administrative scheme to ensure that access to information and other assets is correctly managed and that assets are safeguarded. It is not statutory but operates within the framework of domestic law, including the requirements of the Official Secrets Acts (1911 and 1989) (OSA), the Freedom of Information Act (2000)(FOIA), the Environmental Information Regulations (2004) (EIR) and the Data Protection Act (1998) (DPA). All government assets can be classified, although the Scheme mostly applies to information held electronically or in paper documents.

Key Principles

The Security Classifications has four key principles:

ALL information that government needs to collect, store, process, generate or share to deliver services and conduct government business has intrinsic value and requires an appropriate degree of protection.

EVERYONE who works with or within government (including staff, contractors and service providers) has a duty of confidentiality and a responsibility to safeguard any government information or data that they access, irrespective of whether it is marked or not, and must be provided with appropriate training.

Access to information must **ONLY** be granted on the basis of a genuine **"need to know"** and with appropriate security controls.

Information and other assets received from or exchanged with external partners **MUST** be protected in accordance with any relevant legislative or regulatory requirements, including any international agreements and obligations.

What about existing / legacy information?

The new scheme only applies to information created from 2 April 2014 onwards. There is no requirement for you to undertake an exercise to reclassify all your information. However, if in the line of your routine work you have to revisit / revise older documents you should consider applying the new classification to them.

3. Working with Security Classifications

OFFICIAL

ALL routine information about public sector business, operations and services should be classified as **OFFICIAL**, NICS Departments and Agencies will routinely operate at this level. There is no requirement to explicitly mark routine **OFFICIAL** information. Information which has not been marked is automatically considered **OFFICIAL**.

OFFICIAL includes a wide range of information, of differing value and sensitivity, which needs to be defended against the threat of compromise, and to comply with legal, regulatory and international obligations. This includes:

- The day to day business of government, service delivery and public finances.
  - E-mails on NICS systems
  - Documents on NICS Records Management Systems
  - NICS physical files (paper)
- Routine international relations and diplomatic activities.
- Public safety, criminal justice and enforcement activities.
- Many aspects of defence, security and business continuity.
- Commercial interests, including information provided in confidence and intellectual property.
- Personal information that is required to be protected under the DPA, EIR or other legislation (e.g. health records). (See Appendix 1 FAQ's - Working with Personal Information).

Consult with your Departmental Information Manager (DIM), Assistant Departmental Security Officer (ADSO) or Information Technology Security Officer (ITSO) if you require further guidance.

3. Working with Security Classifications (cont'd)

Handling Indicators

Almost all personal information/data will be handled within **OFFICIAL** without any caveat or descriptor. In limited circumstances, specific considerations may warrant the use of special handling indicators in conjunction with the **OFFICIAL** classification marking to indicate the nature or source of its content, limit access to designated groups, and / or to signify the need for enhanced handling measures and reinforce the "need to know" principle.

OFFICIAL-SENSITIVE

In some instances a very limited need to know must be enforced and a single handling caveat **OFFICIAL-SENSITIVE** provides for this. The handling caveat **OFFICIAL-SENSITIVE** should be used in very limited circumstances where there is a clear and justifiable requirement to reinforce the "need to know" as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for government more generally.

OFFICIAL-SENSITIVE might include, but is not limited to the following types of information:

- The most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- Policy development and advice to ministers on contentious and very sensitive issues;
- Commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to the NICS or to a commercial partner if improperly accessed;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- More sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but does not require **SECRET** level protections;
- Diplomatic activities or negotiating positions where inappropriate access could impact foreign relations or negotiating positions: and
- Very sensitive personal data, where it is not considered necessary to manage this information in the **SECRET** tier.

3. Working with Security Classifications (cont'd)

Extra care needs to be taken when handling the small amount of NICS information within the **SENSITIVE** category. As well as general handling of **OFFICIAL**, this also means:

- ✓ Send the information by the secure NICS email route or use encrypted data transfers.
- ✓ Use recognised commercial couriers if sending hard copy and tamper evident envelopes.
- ✓ Store information securely when not in use and use an approved security cabinet.
- ✓ Only use approved encrypted devices to store information (see NICS Laptop and Mobile Device Security Policy).
- ✓ If faxing the information, make sure the recipient is expecting your fax and check their fax number.
- ✓ Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details.
- ✓ Only print where absolutely necessary.
- x Do not send **OFFICIAL-SENSITIVE** information to internet email addresses, eg. gmail, Hotmail.

3. Working with Security Classifications (cont'd)

Descriptors

DESCRIPTORS may be applied to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes. Descriptors should be used in conjunction with a security classification and applied in the format: **OFFICIAL-SENSITIVE [DESCRIPTOR].**

Descriptors must support the "need to know" principle and help those handling information to consider what group of people either should or should not have access to it. They do not indicate an additional level of security; it is the classification that determines the level of protection. The Descriptors used may include, but are not limited to:

COMMERCIAL: Commercial-or market-sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to HMG/NICS or to a commercial partner if improperly accessed.

PERSONAL: Particularly sensitive information relating to an identifiable individual, where inappropriate access could have damaging consequences. For example, where relating to investigations, vulnerable individuals, or the personal / medical records.

INVESTIGATION: Concerning investigations into disciplinary or criminal matters including information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases. (see information relating to enforcement activity).

LEGAL: Information in connection with any legal proceedings (including prospective legal proceedings), for obtaining legal advice or for establishing, exercising or defending legal rights.

EXECUTIVE: Draft and final versions of Executive Memorandums; minutes of Executive meetings; and correspondence between a Minister and Executive colleagues. **OFFICIAL-SENSITIVE EXECUTIVE** may be used where the subject matter requires it.

Descriptors must not be applied to information that is sent to overseas partners (unless formally agreed in advance) as they are not recognised under any international agreements and are likely to cause confusion.

Access to sensitive information or assets must only be granted to those who have a business need. This "need to know" principle is fundamental to the security of all NICS assets which is based on the classification scheme. If there is any doubt about giving access to sensitive assets individuals should consult their Information Asset Owner (IAO) or ADSO before doing so.

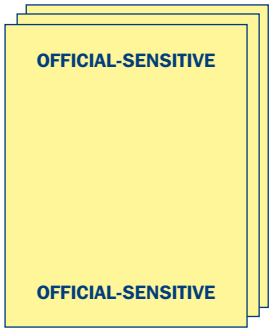
3. Working with Security Classifications (cont'd)

Marking OFFICIAL-SENSITIVE Information

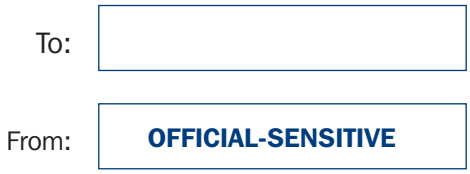
Security classifications can be added to information in many different ways but the most important thing is that the marking is clearly visible to anyone using or receiving the information.

This will mean:

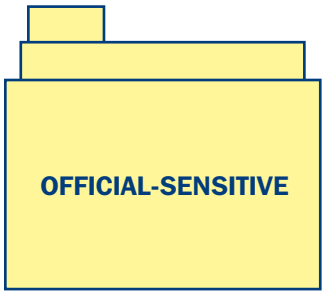
The top and bottom of documents



The subject line or body of emails



The front of folders or binders



It is your responsibility to find out how you are required to mark information but remember OFFICIAL-SENSITIVE information must <u>always</u> be marked.

Frequently Asked Questions

Further information addressing practical aspects of working with the **OFFICIAL** and **OFFICIAL-SENSITIVE** levels of the Government Security Classifications Policy is provided at:

Appendix 1- FAQ1: Working with Personal Information

Appendix 2 - FAQ2: Working with Official Information

Appendix 3 - FAQ3: Security Handling, Controls And Outcomes Tables

3. Working with Security Classifications (cont'd)

SECRET AND TOP SECRET

There is a materially different threshold for **SECRET** assets, both in terms of threat and the impact of compromise. Pre April 2014 **RESTRICTED** (or **CONFIDENTIAL**) information should only move into the **SECRET** tier if the SIRO has been assured that BOTH the consequences of compromise or loss correspond to the impact statements set out in the HMG classification policy; AND that the information needs to be defended against highly capable, determined and well resourced threat actors. If you think that **SECRET / TOP SECRET** classifications are required please seek further guidance from your ADSO.

4. Additional Considerations

When working with information assets, the following points need to be considered:

- Information (and other assets) must be protected in line with the requirements of the classification scheme throughout their lifecycle from creation to destruction to ensure a proportionate level of protection;
- Applying too high a marking can inhibit sharing and lead to unnecessary and expensive protective controls;
- Applying too low a marking may result in inappropriate controls and potentially put sensitive assets at greater risk of compromise;
- It is good practice to reference the classification in the subject line and / or text of email communications. If available you should select a classification before sending, e.g. via a drop-down menu;
- Only originators can classify an asset or change its classification, though holders of copies may challenge it with a reasoned argument. Every effort should be made to consult the originating organisation before a sensitive asset is considered for disclosure, including release under FOIA, EIR, DPA or to the Public Record Office of Northern Ireland;
- A file, or group of sensitive documents or assets, must carry the highest marking contained within it. For example, a paper file or an e-mail string containing **OFFICIAL** and **OFFICIAL-SENSITIVE** material must be covered by the higher marking (i.e. **OFFICIAL-SENSITIVE**);
- E-mails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an e-mail "string" before they add to it and forward it on;
- In certain circumstances there may be a good reason to share selected information from a sensitive report more widely. Originators should consider whether it is possible to develop a sanitised digest or pre-agreed form of words at a lower classification in anticipation of such a requirement;
- Where practicable, time-expiry limits should be considered so that protective controls do not apply for longer than necessary, this is particularly the case for embargoed material intended for general release and only sensitive until it is published, e.g. official statistics;
- Where information is shared for business purposes departments and agencies must ensure the receiving party understands the obligations and protects the assets appropriately.

4. Additional Considerations (cont'd)

- Assets sent overseas must be protected by appropriate national prefixes, caveats and / or special handling instructions. Assets received from overseas nations or international organisations must be protected in accordance with treaty obligations or afforded the same protection as equivalent UK assets if no formal agreement is in place;
- All staff handling sensitive information must be briefed about how legislation (particularly the OSA, FOIA, EIR and DPA) specifically relates to their role, including the potential disciplinary or criminal penalties that may result from failure to comply with security policies. Appropriate management structures must be in place to ensure the proper handling, control and (if appropriate) managed disclosure of sensitive assets; and
- For new policies or projects that include the use of personal information all departments must assess the privacy risks to individuals in the collection, use and disclosure of the information and a **Privacy Impact Assessment (PIA)**, as recommended by the Information Commissioner, should be carried out as a minimum.

Destruction of paper records

Care must be taken when destroying NICS paper records. The basic procedures for destruction are:

OFFICIAL (Non-sensitive records)	**OFFICIAL-SENSITIVE**
Files/records not normally available to the public: shredded and bagged for collection by approved disposal firm; Information in public domain: treat as ordinary waste for recycle bin.	Shredded and / or bagged for collection by approved disposal firm; consider cross-cut shredded and /or bagged for pulping or burning by approved disposal firm for particularly sensitive items.

5. Need to Know Principle

The dissemination of information and assets should be no wider than is necessary for the efficient conduct of an organisation's business and, by implication, should be limited to those individuals who are appropriately authorised to have access to it. This "need to know" principle is fundamental to the protection of government information. It applies both within a Department or Agency and when dealing with individuals outside it.

Departments and Agencies must ensure that individuals are made fully aware of their personal responsibility to apply the "need to know" principle within their own area of activity. This principle should be applied robustly when information is being circulated. Staff should be instructed that if there is any doubt about giving access to official sensitive information to other individuals or organisations they should consult their line manager, IAO or ADSO.

Originators of a circulation list that covers more than one department should ensure that it includes both the name and the department of each individual on the list.

Reproduction of information e.g. by photocopying or an electronic document forwarded by email, should be kept to an absolute minimum and such material should not be copied to other staff as a matter of routine unless they have a "need to know".

6. Working with Personal Data

When handling personal data you need to be particularly careful to ensure compliance with the requirements of the DPA. If you require further information please consult with your line manager, IAO, or DIM.

7. Clear Desk Policy

A Clear Desk Policy reduces the risk of a security breach, fraud or information theft caused by sensitive information being left unattended in the office; and requires Departmental assets, including documents, laptops, blackberries, iron-keys, mobile phones, cameras and all other removable objects of value, are to be locked away when the office is unattended.

A Clear Desk Policy must operate in all offices. Line Managers should make arrangements for systematic room checks to be carried out at the end of each day. A clear desk at the close of work is an important security practice and it is the responsibility of staff and managers to ensure that material cannot be overlooked, handled or removed by unauthorised personnel. At the end of each working day all staff should clear their desks and immobilise office equipment which is not required to be utilised outside of office hours. Line Managers should also carry out periodic checks to ensure procedures are being adhered to.

Furniture

OFFICIAL or **OFFICIAL-SENSITIVE** material can normally be securely stored in ordinary lockable wooden or metal office furniture. Approved security furniture may be required for the storage of some **OFFICIAL-SENSITIVE** information where compromise or loss could have significant consequences for the Department. Requests for security furniture must be made through the ADSO and must be accompanied by a brief business case.

8. Working Away from the Office

Be aware of the increased responsibility which remote working imposes in respect of duty of care towards assets and information. It is your responsibility to decide on whether or not the location is suitable for remote working. If you are required to regularly work remotely you should obtain permission from the manager of your business area. If permission is granted:

- Take only the minimum documentation or information required and record in line with Departmental Policy;
- Keep information secure at all times;
- You must only use a NICS-owned and supported PC or laptop which has NICS approved encryption;
- Do not allow family, friends or others to use official equipment (PC, laptop, PDA, mobile phone etc.);
- Take care when sending and receiving emails and fax messages from remote locations;
- When working remotely be aware that what you say could be heard by others and repeated innocently to someone else;
- Return papers and computer media to your office for proper disposal;
- Laptops should be contained within a locked area when not in use and secured using an appropriate laptop cable lock;
- Laptops and information must be protected in transit and in accordance with NICS Laptop Security Policy and Mobile Device Security Policy.

In public areas be careful to prevent others overlooking your work or overhearing conversations on business related matters. Do not use the IT facilities of any company you visit for official business.

Before working outside the UK with NICS assets, you must obtain Grade 5 approval and you must also inform the ADSO and ITSO so that s/he can ensure the Crypto Custodian is notified.

Only NICS provisioned Secure Remote Access (SRA) facilities on a NICS laptop can be used to gain access to NICS systems from outside the regular office environment. Further guidance on working away from the office can be found in the **NICS Laptop and Mobile Device Security Policy**.

9. Using Electronic Communication - Email

Electronic communication is an integral part of many civil servants' lives, but careless or negligent use can lead to complaints or legal proceedings against NICS Departments or you as an individual employee.

We use electronic communication to communicate with colleagues, other organisations, our customers and members of the public, in a responsive, fast and flexible way. You should however familiarise yourself with the NICS policy set out in the **HR Handbook: Use of Electronic Communications**

Examples of electronic communication include use of the internet, instant messaging, SMS/ MMS or social networking, but the most commonly used method of electronic communication throughout the NICS is email.

- Staff may send emails containing information up to **OFFICIAL–SENSITIVE** to:

- another NICS officer using their standard email address in the format

  forename.surname@departmentni.gov.uk

- a GB department which is connected to the Government Secure Intranet (GSI) provided it is sent to its email address in the GSI format.

  forename.surname@department.gsi.gov.uk

Before sending any email to addresses other than those specified above, staff must consider carefully the information contained both in the body of the message and in any attachments.

Personal or sensitive information is not suitable to be sent over an unauthorised network, e.g. the internet, without protection by NICS approved encryption. The ITSO will be able to assist you with encryption.

- Staff should reference the classification in the subject line and / or text of email communications;
- If both OFFICIAL and **OFFICIAL-SENSITIVE** documents are contained in an email the higher classification should be included in the subject line;
- Emails are often conversational documents, added to by several people in response to a query or question. Individual recipients must assess the entire contents of an email "string" before they add to it or forward it on;
- Particular care should be taken when adding an address to an email. When you start to type in the name of the recipient, NICS "Active Directory" will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg "Dave" - the auto-complete function may bring up several "Daves". Make sure you choose the right address before you click send.

9. Using Electronic Communication - Email (cont'd)

Receiving Email

If you are expecting to receive personal or other sensitive information via email from another public body, you should always ensure that it is sent to you using a secure network i.e. in the gsi or pnn format forename.surname@departmentni.gsi.gov.uk. The NICS email system will remove the gsi and forward the message to your standard NICS email address.

Private Email Addresses and use of Blind Carbon Copy (BCC)

A private email address is considered to be personal data where it can identify a living individual. It is therefore a security breach if you disclose someone's personal email to another 3rd party without the permission of the email owner. If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

Distribution Lists

Distribution Lists (or group email addresses) can be a very good way of saving time and effort. However, be careful when using them. Check who is in the Distribution List and make sure you really want to send your message to everyone.

Personal Use

You may make occasional use of your official departmental/Agency email account to send, forward or receive personal emails. You should however familiarise yourself with the NICS policy set out in the HR Handbook: Use of Electronic Communications.

10. Using Fax

Before using Fax consider whether sending the information by other means is more appropriate, such as using a courier service or secure email. Make sure you only send the information that is required. If you must use a Fax machine:

- Use a cover sheet i.e. a page of explanation sent as the first page of the fax transmission. It must specify who the intended recipient is, the total number of pages in the fax, the subject matter of the fax, and provide the sender's details. This will clearly show who the information is for and whether it is **OFFICIAL-SENSITIVE**, without the receiver having to look at the contents;
- Make sure you double check the fax number you are using. It is best to dial from a directory of previously verified numbers;
- Check that you are sending a fax to a recipient with adequate security measures in place. For example, your fax should not be left uncollected in an open plan office;
- If the fax is personal or other sensitive information, ask the recipient to confirm that they are at the fax machine, they are ready to receive the document, and there is sufficient paper in the machine **before** you send;
- Ring up or email to make sure the whole document has been received safely.

11. IT security - 10 Key Rules

Here are the 10 key rules that all NICS civil servants must follow to ensure the security of personal data:

1. Staff who use a portable device are personally responsible for its safekeeping and for the security of any information it contains.
2. Be very careful with personal or sensitive information and data marked **OFFICIAL–SENSITIVE**. Be especially careful about files which contain large volumes of personal data - e.g. spreadsheets with lists of personal details which may identify or relate to a third party.
3. If you leave any computer switched on and unattended press Ctrl/ Alt/ Delete and select 'Lock Computer'.
4. Sensitive or personal data must not be stored on a laptop unless it is encrypted. This should be stored on TRIM which is adequately secure. An encrypted laptop is one that needs an Ironkey to start-up.
5. Sensitive or personal data must not be stored on mobile phones or removable media unless encrypted. Removable media include USB data drives, external hard drives, CDs, or multi-media data storage cards. The only encrypted removable media approved for use by NICS is the USB data drive. The only encrypted mobile phone is a Blackberry.
6. During office hours, laptops must not be left unattended unless firmly secured with a cable lock.
7. Outside office hours, laptops that are left in the office must be stored in a suitable locked cabinet. Cable locks are not secure out of hours.
8. Be very careful if you take your laptop or portable device out of the office. Take special care in public, at airport security checks, in cars, in hotel rooms and at conferences or meetings.
9. Encrypted laptops and Blackberries are secure, but you must still take great care of them. First of all they are high-cost and valuable items, but also if they are lost or stolen there will be a perception that sensitive or personal data has been compromised.
10. Exceptions to these rules can only be made in the most exceptional circumstances and then only if approved in writing by a Grade 5 with a copy to the ADSO.

All information is susceptible to many types of compromise, but the information which we hold on our computer systems is susceptible to an even greater range of threats.

12. Further Information and Useful Links

Further advice and information on Physical, Document and IT Security can be obtained from your ADSO and DIM. Your ITSO will be able to assist with IT security matters.

NICS Material

The New Government Classification Scheme In line with the rest of the UK the NICS is changing the way it classifies and protects its information. The Cabinet Office has developed a new Government Security Classification scheme, which in order to maintain access to Whitehall systems/services, devolved administrations will be required to use from April 2014.

HMG Material

Government Security Classifications April 2014 – Cabinet Office Guide

FAQ Managing Information Risk at OFFICIAL - This FAQ is intended to help organisations and risk owners understand how ongoing and future risk management activities should be conducted under the new Classification Policy. It will also outline the typical circumstances where OFFICIAL information can be securely managed on specific types of ICT infrastructure.

Introducing the Government Security Classifications - Core briefing for 3rd Party Suppliers

Government Security Classifications Supplier Slides Oct 2013 - Slides - Core Brief for 3rd Party Suppliers

Appendix 1 - FAQ 1: Working with Personal Information

This FAQ sheet addresses practical aspects of working with personal information and data using the Government Security Classifications Policy i.e. **OFFICIAL**, **OFFICIAL-SENSITIVE** and **OFFICIAL–SENSITIVE PERSONAL** levels.

Will all personal information be handled in OFFICIAL?

Almost all personal information/data will be handled within **OFFICIAL** without any caveat or descriptor. In very limited circumstances, specific sensitivity considerations may warrant additional (generally procedural) controls to reinforce the "need to know" for access to certain personal data at **OFFICIAL**.

What type of personal information might qualify as OFFICIAL-SENSITIVE?

It is NOT intended that because an **OFFICIAL** document or data contains personal information it should be routinely marked **OFFICIAL-SENSITIVE**, it should meet the criteria set out below.

The **OFFICIAL-SENSITIVE** (and **OFFICIAL-SENSITIVE PERSONAL**) caveat should **ONLY** be applied where the "need to know" must be most rigorously enforced, particularly where information may be being shared outside of a routine or well understood business process. For example, where the loss or compromise of information could have severely damaging consequences for an individual or group of individuals – including staff - there is a clear and justifiable requirement to reinforce the "need to know" principle.

What about aggregation of large amounts of personal data

Where large data sets of personal information exist in the **OFFICIAL** classification, effective procedural, and in some cases technical, controls may be appropriate to reinforce the "need to know" principle and provide enhanced protection. However the data should not automatically be marked **OFFICIAL-SENSITIVE**.

Can I use a descriptor to identify information or data that contains personal information?

Only in very specific circumstances to identify certain categories of information that have already been assessed **OFFICIAL-SENSITIVE**.

The descriptor should be applied in the format: **OFFICIAL-SENSITIVE PERSONAL**

Can I send OFFICAL documents containing personal information across the Internet or email them to people on the Internet?

Electronic communication is an integral part of many civil servants' lives, but careless or negligent use can lead to complaints or legal proceedings against NICS Departments or you as an individual employee. You must not send personal information across the internet unless it is protected by NICS encryption. Further information can be obtained from your ITSO.

Appendix 1 (cont'd)

Can personal information be off shored?

Any organisation planning to store or process personal information / data outside the UK/EEA must first consult the Departmental Senior Information Risk Owner (SIRO) who can seek advice from Office of the Government SIRO (OGSIRO).

Does **OFFICIAL-SENSITIVE** personal information have to be registered and tracked?

Where large volumes of **OFFICIAL-SENSITIVE** personal information or data are regularly shared between organisations, the respective SIROs and IAOs may wish to agree specific handling arrangements and transfer protocols in line with their departmental policies. Any personal data regularly shared by NICS Departments/Agencies/NDPBs should only take place where a formal Data-Sharing Agreement has been drawn up and approved.

What about meeting the Data Protection Act requirements?

The DPA requirement to provide appropriate and proportionate protection for personal data is unchanged. SIROs and IAOs need to assure themselves that they have taken reasonable steps to comply with the DPA principles. Organisations must ensure that staff are trained in the handling of any personal data they process or manage and that tailored guidance is available about specific local processes. Security Classifications are designed to be used in parallel with any DPA controls but will not in themselves provide the requisite protection for information covered by DPA.

How should business areas deal with personal information losses or breaches?

Just as they do now. Each Department will have its own information loss handling procedure aligned to the NICS procedure for handling losses of personal data.

Staff must also ensure that they complete any relevant training to ensure they are handling personal data in line with this policy and the DPA.

What about sensitive personal data as defined by the DPA?

In most cases (apart from where other particular sensitivity considerations apply) personal data and sensitive personal data, as defined by the DPA, will be handled within **OFFICIAL** without any caveat or descriptor. If you require further information please consult with your line manager, IAO, or DIM.

Appendix 1 (cont'd)

Will personal information in the **OFFICIAL** level be widely accessible?

No. All information must be subject to appropriate protection. There is no presumption of unbounded access at any level of the classification policy; though the principles of openness, transparency and information reuse need to be considered. As with current arrangements, the NICS should use ICT access control measures, supported by procedural and personnel controls, to manage their information assets and enforce the "need to know" principle.

All personal data / information is subject to the "need to know" principle and it is the responsibility of IAOs to ensure that this is enforced in respect of personal data / information for which they are responsible.

Will the **OFFICIAL** level provide the adequate/proper protection for personal data?

Everyone working with government information, staff, contractors and service providers, has a personal responsibility to safeguard any NICS / HMG information or data that they access, irrespective of whether it is marked or not.

IAOs need to consider the sensitivity and threats to their information and to identify those instances where access to personal information must be no wider than necessary for the efficient conduct of an organisation's business. The "need to know" principle must be used wherever personal information is collected, stored, processed, destroyed or shared within government and when dealing with external public or private sector organisations, and effective procedural controls put in place.

Is there a single set of baseline security controls that will protect all personal data?

No, as currently the controls will vary according to a range of factors, for example the value and sensitivity of the information, the threats to that information, how it is used, by whom and where. The NICS needs to undertake a holistic risk assessment to determine the appropriate controls necessary to meet the confidentiality, integrity and availability requirements.

Appendix 2 - FAQ2: Working with Official Information (General Guidance)

This FAQ sheet addresses practical aspects of working with the OFFICIAL (including OFFICIAL-SENSITIVE) level of the Government Security Classifications Policy.

General Principles

The NICS holds a very wide range of information and delivers many different services, but many of the information risks across Business Areas are broadly similar. The majority of information related to NICS business, operations and services can be managed as **OFFICIAL**. Indeed most Business Areas will operate almost exclusively at this level. There is no unclassified level below **OFFICIAL** - any information that is created, processed, generated, stored or shared within (or on behalf of) NICS is **OFFICIAL** by definition. There is no requirement to mark routine **OFFICIAL** information.

Personnel, physical and information security controls for **OFFICIAL** are based on commercial good practice, with an emphasis on staff to respect the confidentiality of all information. In some instances a more limited "need to know" must be enforced and assured. A single handling caveat **'OFFICIAL-SENSITIVE'** provides for this. **OFFICIAL–SENSITIVE** material must be clearly marked.

Descriptors

Descriptors distinguish specific types of information; they do not attract additional security controls per se and should be used in conjunction with a security classification applied in the format: **OFFICIAL-SENSITIVE [DESCRIPTOR]**

Descriptors will distinguish specific types of information in the following circumstances:

- To distinguish commercial or market sensitive data, including that subject to statutory or regulatory obligations, that may be damaging to NICS / HMG or to a commercial partner if improperly accessed;
- To identify particularly sensitive information relating to an individual (or group), where inappropriate access could have damaging consequences;
- The use of descriptors is at an organisation's discretion. But where they have been applied by an originator, they should be carried forward.

Staff may apply Descriptors to identify certain categories of sensitive information and indicate the need for common sense precautions to limit access. Where descriptors are permitted they must be supported by local policies and business processes.

Appendix 2 (cont'd)

Information relating to enforcement activity

NICS holds a limited range of information around enforcement and legal advice the majority of which will be managed as **OFFICIAL**. However within this category of information there will be instances where a more limited "need to know" must be enforced and assured. Staff need to think about the nature and context of any information they handle when deciding whether it is appropriate to particularly enforce need to know through use of the **OFFICIAL-SENSITIVE INVESTIGATION** caveat. The handling caveat **OFFICIAL–SENSITIVE INVESTIGATION** must be clearly marked.

Information relating to legal advice

NICS holds a limited range of information around legal advice the majority of which will be managed as **OFFICIAL**. However within these types of information there will be instances where a more limited need to know must be enforced and assured. The handling caveat **OFFICIAL–SENSITIVE LEGAL** must be clearly marked.

Using the new markings

How does the OFFICIAL classification map to the existing Government Protective Marking Scheme (GPMS)?

There is no direct correlation between the new classification policy and the old GPMS scheme. In general terms, assets that were previously classified up to and including **RESTRICTED** should be managed at **OFFICIAL**.

Business Areas need to think about the nature and context of any information they handle when deciding whether it is appropriate to particularly enforce "need to know" through use of the **OFFICIAL-SENSITIVE** caveat.

Business Areas need to consider the sensitivity and threats to their information. In most cases, all formerly **RESTRICTED** marked material should be managed as **OFFICIAL** with appropriate procedural controls to enforce need to know restrictions.

Whilst the controls at **OFFICIAL** (e.g. 'good' commercial ICT products and services) cannot absolutely assure against the most sophisticated threats, they will provide for robust and effective protections that make it very difficult, time consuming and expensive to illegally access this information. In this respect it is no different from pre April 2014 arrangements for the classification levels of **PROTECT** and **RESTRICTED**.

Appendix 2 (cont'd)

There is a materially different threshold for **SECRET** assets, both in terms of threat and the impact of compromise. Pre April 2014 **RESTRICTED** (or **CONFIDENTIAL**) information should only move into the **SECRET** tier if the SIRO has been assured that BOTH the consequences of compromise or loss correspond to the impact statements set out in the HMG classification policy; **AND** that the information needs to be defended against highly capable, determined and well resourced threat actors. If you think that **SECRET / TOP SECRET** classifications are required please seek further guidance from your ADSO.

Will information in the OFFICIAL level be widely accessible?

No. There is no presumption of disclosure or unbounded access at any level of the classification policy; though the principles of openness, transparency and information reuse require that individuals consider the proactive publishing of information and data sets where appropriate.

Staff should use proportionate ICT and paper document access controls, supported by procedural and personnel controls, to manage their information assets and enforce need to know restrictions.

Is there an unclassified tier below OFFICIAL?

No, the new classification scheme has quite purposefully taken the pre April 2014 UNCLASSIFIED caveat out of the equation. ALL information that is created, collected, processed, stored or shared within government (and across the wider Public Sector) has value and must be handled with due care. This includes published data where integrity and availability considerations (and often Crown Copyright) may continue to apply.

Staff are expected to think about the nature and context of the information they work with and to exercise good judgement to ensure that all information (and other assets) is handled and safeguarded appropriately.

Many staff will use publically available information in their work (e.g. raw data from the internet). However, there is no requirement for an 'unclassified' infrastructure to manage this information as anything that staff create or process is by definition **OFFICIAL**.

What is the threshold for using the caveat OFFICIAL-SENSITIVE?

All staff should use their discretion to determine those instances where it will be appropriate to use the **OFFICIAL-SENSITIVE** caveat as this will vary depending on the subject area, context and in some cases, any statutory or regulatory requirements.

Appendix 2 (cont'd)

Staff need to make their own judgements about the value and sensitivity of the information that they manage, in line with departmental and corporate risk appetite decisions. However, the handling caveat should be used by exception in limited circumstances where there is a clear and justifiable requirement to reinforce the "need to know" as compromise or loss could have damaging consequences for an individual (or group of individuals), an organisation or for NICS / HMG more generally. This might include, but is not limited to the following types of information:

- the most sensitive corporate or operational information, e.g. relating to organisational change planning, contentious negotiations, or major security or business continuity issues;
- policy development and advice to ministers on contentious and very sensitive issues;
- commercial or market sensitive information, including that subject to statutory or regulatory obligations, that may be damaging to NICS / HMG or to a commercial partner if improperly accessed;
- Information about investigations and civil or criminal proceedings that could compromise public protection or enforcement activities, or prejudice court cases;
- more sensitive information about defence or security assets or equipment that could damage capabilities or effectiveness, but does not require **SECRET** level protections;
- diplomatic activities or negotiating positions where inappropriate access could impact foreign relations or negotiating positions and must be limited to bounded groups;
- very sensitive personal data, where it is not considered necessary to manage this information in the **SECRET** tier.

Managers within Business Areas should ensure that staff are trained to understand the sensitivities related to the information they work with (including any statutory or regulatory requirements), supported by local business processes, and instructed about the need to provide meaningful guidance when sharing that information with others.

How should personal data be managed?

Handling personal data is covered separately in APPENDIX 1 - FAQ1: Working with Personal Information.

Appendix 2 (cont'd)

How should UK information that is sent overseas be marked?

Detailed guidance on the equivalencies between UK and international classification schemes, and any supplementary handling or protection requirements, is provided in separate guidance. In general terms, any sensitive NICS / HMG information that is shared with international partners must be marked with the 'UK' prefix to identify the originator and provide a measure of protection under partners' freedom of information legislation.

How should time-sensitive information be managed?

Staff should be encouraged to provide meaningful guidance on handling any sensitive information that they share, including if sensitivities are time-bound and information can be distributed more widely after a particular date or event, e.g. in the case of official statics or the Budget. The Classification Policy does not mandate a format for such guidance.

Who can mark / unmark a document?

The originator is responsible for determining the appropriate classification for any assets they create, though recipients / holders of copies may challenge the classification with a reasoned argument if necessary. Depending on context and circumstances sensitivities may change over time and it may become appropriate to reclassify an asset.

Every effort should be made to consult the originator or originating organisation before a sensitive asset is considered for disclosure, including release under the FOIA, EIR or to the Public Record Office. Where the originating organisation cannot be identified (e.g. following Machinery of Government changes) it is good practice to consult with copy recipients.

Where an asset is originated by a foreign government or international organisation, the originator must always be consulted before the asset can be remarked or disclosed to an individual that does not hold the appropriate personnel security control.

Does existing information need to be remarked?

No. As a rule, organisations are not required to retrospectively remark legacy information or data that uses the old protective markings. Nor does information or data need to be remarked where it is in continued use within an organisation, provided that users / recipients understand how it is to be handled in line with the Classification Policy.

However, where legacy information or data bearing a former protective marking is to be shared or exchanged between organisations, or with external partners, the originator should consider remarking with the appropriate security classification. At the very least, meaningful guidance should be provided about how the asset should be protected in line with the new approach.

Appendix 2 (cont'd)

Who can I go to for advice on valuing my information assets?

Information within the NICS is the responsibility of IAOs. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide advice to the SIRO on the security and use of their information.

Appendix 3 - Security Handling, Controls and Outcomes

Handling OFFICIAL

Handling

✓ Handle OFFICIAL information with care.

✓ Apply the clear desk policy.

✓ Comply with all legal and regulatory obligations and follow NICS policies and standards.

! How sensitive is the information you handle? This forms the basis for your judgment on how to share and protect it.

Sharing

✓ Responsible information sharing, with the right people, is vital to the provision of public services.

✓ Use NICS email systems to share information to ensure traceability.

✓ Take extra care when sharing information with external partners or the public - send to named recipients at known addresses.

✓ Explain to recipients any particular information handling requirements. Eg. who can see it? Is it sensitivity time limited?

✓ Encrypt all information stored on removable media.

! Is your information suitable to send to internet email addresses eg. gmail or Hotmail, or is it too sensitive?

! Consider extra protection for bulk data transfers. Who needs to approve these?

Protecting

✓ Lock **OFFICIAL** assets away when not in use and lock your screen before leaving your computer unattended.

✓ Protect the **OFFICIA**L assets you take away from the office in proportion to their sensitivity.

✓ Make sure documents are not overlooked when working remotely or in public areas.

✓ Use discretion when discussing information in public or by telephone, keeping sensitive information to a minimum.

! Consider what protection you need for documents taken out of the office - eg. secure brief case, encrypted device.

x Do no leave NICS assets unattended in public.

Disposal

✓ All staff should ensure that they apply the relevant retention and disposal policies when disposing of hard copy or electronic documents.

✓ IT assets must be disposed of in line with NICS secure disposal policy.

Reporting

✓ Report any theft, loss or inappropriate access of information to your Line Manager and the ADSO.

Appendix 3 (cont'd)

Handling OFFICIAL-SENSITIVE

Extra care needs to be taken when handling the small amount of NICS information witthin the **SENSITIVE** category. As well as general handling of **OFFICIAL**, this also means:

- ✓ Send the information by the secure NICS email route or use encrypted data transfers.
- ✓ Use recognised commercial couriers if sending hard copy and tamper evident envelopes.
- ✓ Store information securely when not in use and use an approved security cabinet.
- ✓ Only use approved encrypted devices to store information (see NICS Laptop and Mobile Device Security Policy).
- ✓ If faxing the information, make sure the recipient is expecting your fax and check their fax number.
- ✓ Take extra care to be discreet when discussing sensitive issues by telephone, especially when in public areas and minimise sensitive details.
- ✓ Only print where absolutely necessary.
- x Do not send **OFFICIAL-SENSITIVE** information to internet email addresses, eg. gmail, Hotmail.

Appendix 3 - (cont'd)

Security Controls - OFFICIAL/OFFICIAL-SENSITIVE

Personal Security	Minimum controls include: • Appropriate recruitment checks (e.g. the BPSS or equivalent) • Reinforce personal responsibility and duty of care through training • "Need to know" for sensitive assets
Physical Security Document Handling	• Clear desk/screen policy • Consider proportionate measures to control and monitor access to more sensitive cases
Storage	• Storage under single barrier and/or lock and key • Consider use of appropriate physical security equipment/furniture (see the CPNI Catologue of Security Equipment, CSE)
Remote Working	• Ensure information cannot be inadvertently overlooked whilst being accessed remotely • Store more sensitive assets under lock and key at remote lolcations
Moving assets by hand	• Single cover • Precautions against overlooking when working in transit • Authorisation required for significant volume of records/files
Moving assets by post/courier	• Include return address, never mark classification on envelope • Consider double envelope for sensitive assets • Consider using registered Royal Mail service or reputable commercial courier's 'track and trace' service
Moving assets overseas by hand or post	• Trusted hand under single cover • Consider using reputable commercial courier's 'track and trace' service
Bulk Transfers (volume thresholds may vary by organisation and should be defined in local policies)	• Local management approval subject to departmental policy, appropriate risk assessment and movement plans

Appendix 3 (cont'd)

Security Outcomes - OFFICIAL including OFFICIAL-SENSITIVE

To defend against typical threat profiles, protective security controls achieve the following outcomes:

General Outcomes	• Meet legal and regulatory requirements • Promote responsible sharing and discretion • Proportionate controls appropriate to an asset's sensitivity • Make accidental compromise or damage unlikely
Personnel Security	• Access by authorised individuals for legitimate business reasons
Physical Security (handling, use, storage, transport and disposal)	• Proportionate good practice precautions against accidental or opportunistic compromise • Control access to sensitive assets through local business processes and dispose of with care to make reconstitution unlikely
Information Security (storage, use, processing or tranmission)	• Protect against deliberate compromise by automated or opportunist attack • Aim to detect actual or attempted compromise and respond

Annex A – number of special advisers in other jurisdictions

GB:

https://www.gov.uk/government/publications/special-adviser-data-releases-numbers-and-costs-december-2019

Number of special advisers as at 5 November 2019 - there were 108.4 (full time equivalent) special advisers working across the whole of government. The total Civil Service has 413,910 (full time equivalent) civil servants as at 31 March 2019.

***Appointing Minister Special Adviser / Pay Band Salary Band (If £70,000 or above)**

***The Prime Minister.**

Lee Cain 4 £140,000-£145,000
Dominic Cummings 4 £95,000-£99,999
Nikki Da Costa 4 £125,000-£129,999
David Frost 4 £125,000-£129,999
Andrew Griffith 4 £125,000-£129,999
Oliver Lewis 4 £95,000-£99,999
Sir Ed Lister 4 £140,000-£145,000
Munira Mirza 4 £140,000-£145,000
John Bew 3 £85,000-£89,999
Liam Booth-Smith 3 £85,000-£89,999
Chris Brannigan 3 £85,000-£89,999
Ben Gascoigne 3 £85,000-£89,999
Blair Gibbs 3 £80,000-£84,999
Andrew Gilligan 3 £95,000-£99,999
Jonathan Hellewell 3 £75,000-£79,999
Lucia Hodgson 3 £75,000-£79,999
Tom Irven 3 £85,000-£89,999
Samuel Kasumu 3 £70,000-£74,999
Ross Kempsell 3 £70,000-£74,999
Katie Lam 3 £70,000-£74,999
Douglas McNeill 3 £95,000-£99,999
Tim Montgomerie 3 £80,000-£84,999
Elena Narozanski 3 £75,000-£79,999
Robert Oxley 3 £85,000-£89,999
Meg PowellChandler 3 £85,000-£89,999
Jean-Andre Prager 3 £70,000-£74,999
Sam Richards 3 £70,000-£74,999
Elliot Roy 3 £70,000-£74,999
James Sproule 3 £75,000-£79,999
Will Warr 3 £80,000-£84,999
Cleo Watson 3 £75,000-£79,000
Sheridan Westlake 3 £85,000-£89,999
James Wild 3 £85,000-£89,999

Shelley WilliamsWalker 3 £75,000-£79,999
Ross Allan 2
Rosie Bate-Williams 2
Declan Lyons 2
Marcus Natale 2
Damon Poole 2
Chloe Sarfaty 2
Nick Vaughan 2
Rupert Yorke 2 £70,000-£74,999
Christopher James 1
Chloe Westley 1

***Chancellor of the Exchequer**
Mats Persson 4 £120,000-£124,999
Sam Coates 3 £80,000-£84,999
James Hedgeland 2
Adam Memon 2
Jennifer Powell 2
Tim Sculthorpe 2

***Secretary of State for Foreign and Commonwealth Affairs, First Secretary of State**
Beth Armstrong 3 £80,000-£84,999
Simon Finkelstein 2
Simon Jupp 2
Christina Robinson 2

***Secretary of State for the Home Department**
James Starkie 3 £80,000-£84,999
Hannah Guerin 2
Charlotte Miller 2
Alexander Wild 2

***Chancellor of the Duchy of Lancaster**
Henry Cook 3 £80,000-£84,999
Henry Newman 3 £80,000-£84,999
Josh Grimstone 2
Charles Rowley 2

***Lord Chancellor and Secretary of State for Justice**
Peter Cardwell 2
Rajiv Shah 2

***Secretary of State for Exiting the European Union**
Stephanie Lis 2
Gareth Milner 2
Gavin Rice 2

***Secretary of State for Defence**
Lynn Davidson 3 £80,000-£84,999

***Secretary of State for Health and Social Care**
Emma Dean 2
Allan Nixon 2
Jamie NjokuGoodwin 2

***Secretary of State for Business, Energy and Industrial Strategy**
Samantha Magnus 2
Marc Pooler 2

***Secretary of State for International Trade and President of the Board of Trade, Minister for Women and Equalities**
James Caldecourt 2
Nerissa Chesterfield 2
Sophie Jarvis 2

***Secretary of State for Work and Pensions**
Alex Hitchcock 2
Rhiannon Padley 2

***Secretary of State for Education**
Richard Holden 2
Katherine Howell 2

***Secretary of State for Environment, Food and Rural Affairs**
Saratha Rajeswaran 2 £70,000-£74,999
Robert Rams 2 £70,000-£74,999

***Secretary of State for Housing Communities and Local Government**
Olivia Oates 2
Thomas Kennedy 1

***Secretary of State for Transport**
Emma Barr 2
Rupert OldhamReid 2

***Secretary of State for Northern Ireland**
Ross Easton 2
Lilah HowsonSmith 2

***Secretary of State for Scotland**
Magnus Gardham 2
William Saunders 2

***Secretary of State for Wales**
Geraint Evans 2

***Leader of the House of Lords, Lords Privy Seal**
Annabelle Eyre 3 £80,000-£84,999
Hannah Ellis 1
Yasmin Kalhori 1
James Price 1

***Secretary of State for Digital, Culture, Media and Sport**
Sophia True 2

***Secretary of State for International Development**
Natasha Adkins 2
Will Holloway 2 £70,000-£74,999

***Minister Without Portfolio for the Cabinet Office**
Jessica Prestidge 1

***Chief Secretary to the Treasury**
Claire Coutinho 2 £70,000-£74,999

***Leader of the House of Commons, Lord President of the Council**
Beatrice Timpson 2
Hugh Bennett 1

***Parliamentary Secretary to the Treasury (Chief Whip)**
Sophie Bolsover 2
Simon Burton 2 £75,000-£79,999

***Paymaster General and Minister for the Cabinet Office**
Mike Crowhurst 2
Lucy Noakes 2 £70,000-£74,999

***Minister of State (Minister for the Northern Powerhouse and Local Growth)**
Cameron Brown 2

***Minister of State for Housing**
Daniel El-Gamry 2

*** Minister of State for Security**
Michael Young 2

Welsh Government:

https://gov.wales/written-statement-special-advisers-3

There were 15 Special Advisers in post for all or part of the 2018/19 financial year.
They are appointed by the First Minister to help Ministers on matters where the work of Government and the work of the Government Party overlap and where it would be inappropriate for permanent civil servants to become involved

David Costa **(left on 8/4/18**	- PB2
Kate Edmunds **(left on 12/12/18**	- PB2
Matt Greenough **(left on 12/12/18**)	- PB3
Rachel Maycock (**left on 12/12/18)**	**-** PB2
Huw Price **(left on 12/12/18)**	- PB2
Alex Rawlin **(left on 12/12/18)**	- PB2
Madeleine Brindley	- PB2
Andrew Johnson	- PB2
Jane Runeckles	- PB3
Gareth Williams	- PB3
Tom Woodward	- PB2
David Davies	- PB1
Daniel Butler	- PB1
Paul Griffiths	- PB1
Clare Jenkins	- PB3

PB1 - up to £52,999
PB2 - £53,000 - £69,999
PB3 - £70,000 - £94,999

Scottish Government:

https://www.parliament.scot/parliamentarybusiness/28877.aspx?SearchType=Advance&ReferenceNumbers=S5W-26805&ResultsPerPage=10

14 Special Advisers Financial Year 2018/19

Kathy Bowman – Special Advisor
Culture, Tourism and External Affairs Policy support to the Chief of Staff.
Support for the First Minister and the First Minister's Private Office.
Outreach and stakeholder engagement.

Jeanette Campbell – Special Advisor
Communities, Social Security, and Equalities (apart from Local Government and Planning).

Ewan Crawford – Senior Special Advisor
Europe and Constitutional issues Government Strategy.

Leanne Dobson – Special Advisor
Environment and climate change Land reform.

Kate Higgins – Special Advisor
Rural Economy & Connectivity.
Age of Criminal Responsibility (Scotland) Bill

Davie Hutchinson – Special Advisor
Health & Sport
Broadcasting
First Minister Questions

Ross Ingebrigtsen - Deputy Political Spokesperson for the First Minister
Strategic communications planning

Liz Lloyd - Chief of Staff to the First Minister
First Minister's Strategic Programme in Government including Inter-governmental relations.
Co-ordination of the Special Adviser team.

John MacInnes – Special Advisor
Political Research.
Support for First Minister's Questions and parliamentary debates.
Support to Communications and Policy Special Advisers.

Stewart Maxwell - Special Adviser
Business, the Economy, Skills and Fair Work.
Business and Economy outreach
Veterans

Colin McAllister - Head of Policy
Programme for Government.
First Minister's Questions
Senior Special Adviser to the Deputy First Minister.
Education – apart from Age of Criminal Responsibility (Scotland) Bill.

Callum McCaig - Special Adviser
Finance
Local Government and Planning
Energy

John McFarlane -Special Adviser
Justice
Transport
Parliamentary Business and Parliamentary liaison

Stuart Nicolson - Head of Communications
Senior Political Spokesperson for the First Minister
Strategic communications

Pay band	Pay Range (£)	Number of SpAds in Band
1	39,445 – 52,904	2
2	52,905 – 65,016	6
3	65,017 – 86,964	5
3 (premium)	86,965 - 100,942	0
4	86,965 - 104,462	1

Irish Government:

https://assets.gov.ie/19699/67fe34e66f084372b5f17066e8c8bb75.pdf

58 Special Advisers @ July 2019

Minister Michael Creed - Agriculture, Food & the Marine
Aine Kilroy 14 June 2017 €87,258
Jonathan Hoare 06 May 2016 €79,401
Ultan Waldron 17 October 2017 €81,767

MoS Andrew Doyle

Avril Cronin 02 October 2018 €66,495

Minister Josepha Madigan - Culture, Heritage and the Gaeltacht

John Keogh 08 January 2018 €91,943

Cian Connaughton 01 February 2018 €88,471

Attorney General Seamus Wolfe

Sean Aherne 14 June 2017 €81,767

Minister Katherine Zappon - Children & Youth Affairs

Patricia Ryan 14 June 2017 €85,750

Sinead Fennell 09 July 2019 €85,823

Minister Richard Bruton - Communications, Climate Action and Environment

Sarah O'Neill 16 October 2018 €85,012

Patrick Clusky 16 October 2018 €88,345

Minister Joe McHugh - Education & Skills

Ed Carthy 17 October 2018 €85,823

Mark O'Doherty 17 October 2018 €94,535

MoS John Halligan

Anthony McFeely 29 June 2019 €66,495

MoS Mary Mitchell O'Connor

Roy Dooney 14 June 2017 €94,521

Lynda McQuaid 25 July 2017 €94,521

Minister Michael Ring - Rural & Community Development

Daniel Rowan 14 August 2017 €81,767

Padraig Hughes 11 June 2018 €93,599

Minister Eoghan Murph - Housing, Planning & Local Government

Jack O'Donnell 14 June 2017 €81,767

Jennifer Carroll MacNeill 06 November 2017 €81,767

Minister Simon Coveney - Tanaiste & Foreign Affairs & Trade
Caitríona Fitzpatrick 15 June 2017 €78,670
Matt Lynch 04 December 2017 €88,471
Chris Donoghue 04 December 2017 €98,391
Laura McGonigle 22 July 2019 €92,862

MoS Helen McEntee
Paul Fox 04 September 2017 €65,093

Minister Simon Harris - Health
Joanne Lonergan 14 June 2017 €87,258
Sarah Bardon 20 September 2018 €84,973

MoS Finian McGrath
Gerry Maguirre 14 June 2017 €75,647
Damien O'Farrell 14 June 2017 €79,401

MoS Jim Daly
Darren Hourihan 07 September 2017 €73,846

MoS Catherine Byrne
Nicola Clavin 01 May 2018 €65,837

Minister Heather Humphreys - Business, Enterprise & Innovation
Pauric McPhillips 14 June 2017 €85,091
Lucy Moylan 18 September 2017 €81,767

Minister Charlie Flanegan Justice & Equility
Sean Kavanagh 15 June 2017 €85,091
Caroline Murphy 10 April 2018 €91,943

Minister paschal Donohoe - Finance/Public Expenditure & Reform
Deborah Sweeney 15 June 2017 €88,392
Ed Brophy 12 February 2018 €98,391
Niamh Callaghan 17 May 2018 €84,973

MoS Kevin 'Boxer' Moran
Eugene Deering 03 June 2017 €65,000

MoS Michael D'Arcy
Caroline Hofman 04 June 2019 €66,495

Minister Regina Doherty - Employment Affairs and Social Protection

Denise Duffy 14 June 2017 €81,767
Alex Connolly 01 October 2018 €107,109

Minister Leo Varadkar - Taoiseach and Defence

Angela Flanagan 14 June 2017 €105,000
Brian Murphy 14 June 2017 €157,433
John Carroll 05 July 2017 €128,682
Philip O'Callaghan 14 June 2017 €81,767
Patrick Geoghegan 14 June 2017
Jim D'Arcy 04 September 2017 €74,498
Claire Mungovan 30 January 2018 €88,471

Independent Alliance

Tony Williams 14 June 2017 €94,521
Donal Geoghegan 14 June 2017 €94,521

Sean Kayne Chief Whip

Peter Harper 16 October 2018 €85,823
Peter Feeney 16 October 2018 €85,823

MoS Paul Kehoe - Defence/Taoiseach

Niall O'Connor 29 January 2018 €84,973
John Coughlan 14 June 2017 €79,401

Shane Ross - Transport, Tourism & Sport

Aisling Dunne 15 June 2017 €79,401
Richard Moore 01 July 2019 €85,823
Carol Hunt 15 June 2017 €79,401