BRITISH
TRANSPORT
POLICE

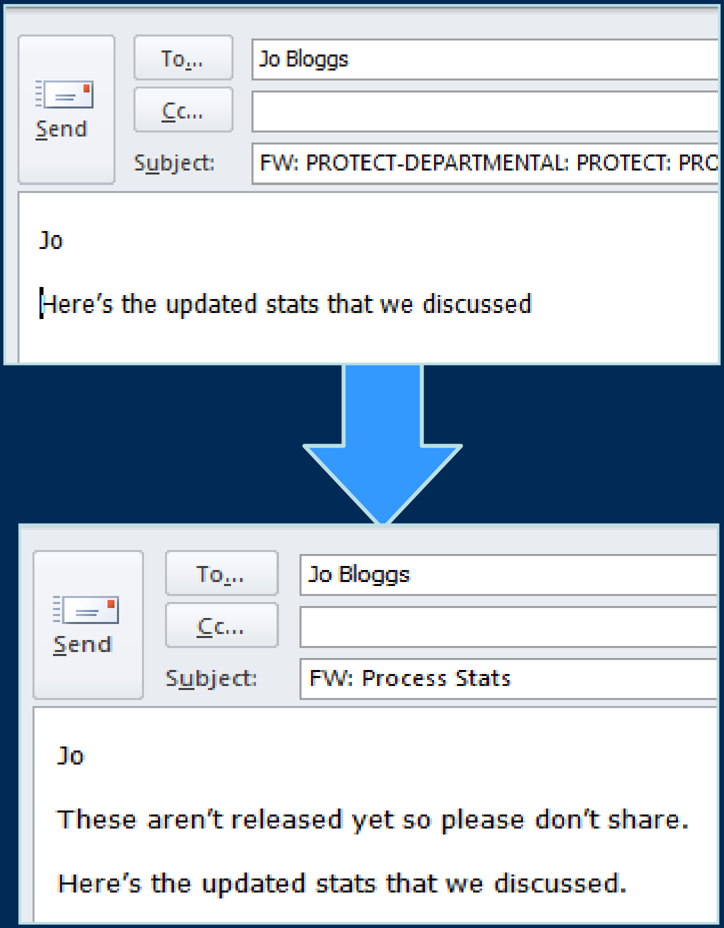
Security Classification Policy
Implementation in Policing – Update

Helen Edwards
Head of Information Management
March 2013

New Security Classifications

BRITISH TRANSPORT POLICE

- From April 2014, the Government security classifications are changing.
- Many organisations that forces work with will be moving to the new classifications This includes CPS, Health and local councils
- Some parts of policing, notably the National Crime Agency, will also adopt the policy.
- Chief Constables Council has agreed in principle to adopt the new classifications, subject to the return of an impact assessment and transition plans to a future meeting.
- It is expected that forces will change over to the new classifications in October 2014.
- Interim guidance will be provided to help forces in the period between April and October 2014.
- It is expected that there will be little or no change to ICT for October 2014.



Subject: FW: PROTECT-DEPARTMENTAL: PROTECT: PRC

To... Jo Bloggs

Jo

Here's the updated stats that we discussed

To... Jo Bloggs

Subject: FW: Process Stats

Jo

These aren't released yet so please don't share.

Here's the updated stats that we discussed.

From Old to New

The old system:

UNCLASSIFIED	PROTECT	RESTRICTED	CONFIDENTIAL	SECRET	TOP SECRET
IL0	IL1/IL2	IL3	IL4	IL5	IL6

The new system:

OFFICIAL	SECRET	TOP SECRET

- Instead of six classifications, there will be three.
- Protective Markings like PROTECT and RESTRICTED will no longer be used
- The removal of UNCLASSIFIED reasserts the fact that **all** Government (and policing) information has value and should be handled with appropriate care.
- There is no direct read-across from the old to new approach.
- Within the **OFFICIAL** classification, a proportion of policing information is sensitive. This will be marked as **OFFICIAL-SENSITIVE**.

OFFICIAL-SENSITIVE

BRITISH TRANSPORT POLICE

- Implementation of the new classifications will be based on the principle that the majority of policing information and data is OFFICIAL.
- It is likely that a significant proportion of operational policing data is OFFICIAL-SENSITIVE, indicating that there are specific information risks to be managed.

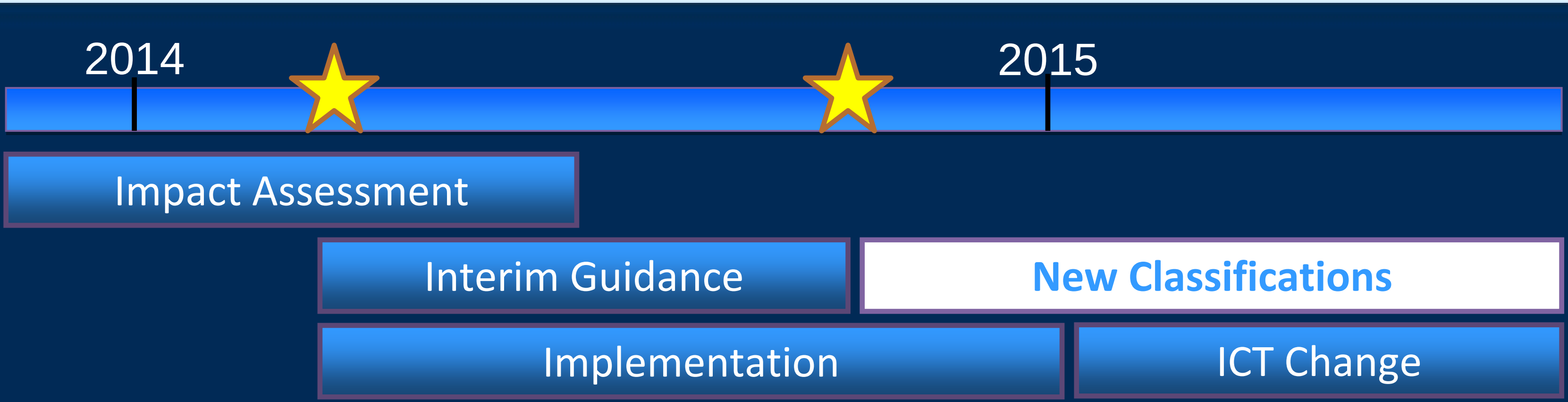
This does not mean that:

- Everything is automatically less secure.
- We automatically take on more risk, or increase our risk appetite.
- Sensitive information automatically becomes **SECRET** (because of a belief that OFFICIAL "isn't secure").
- Documents can automatically be sent by internet email (Gmail, Outlook.com, etc).
- All existing documents and systems need to be reclassified.
- We will take a one-size-fits-all approach to **OFFICIAL-SENSITIVE** information.

This does mean that:

- **OFFICIAL-SENSITIVE** will cover a diverse and varying range of sensitivities, with differing consequences resulting from the compromise or loss of information.
- The context of information and data is important, and there isn't a one-size-fits-all solution.
- A baseline set of controls will be applied.
- Additional controls will be applied based on the specific types of information.
- Handling instructions may need to be given (based on the context).

Implementation Timeline



- **Now**
  - Performing an Impact assessment on priority business processes.
  - Developing interim guidance to be available in time for April 2014.
- **April 2014**
  - Interim guidance in place.
  - Implementation of new classification scheme, including training and communications.
- **October 2014**
  - Policing moves to the new classifications.
- **After October 2014**
  - ICT is changed to maximise benefits of new classification. Changes are made as contracts end or as significant business changes are made.

Interim Guidance

BRITISH TRANSPORT POLICE

- Guidance will be provided to forces on how to handle information in the period between April 2014 and October 2014. In this interim period partner organisations will have adopted the new scheme and policing will continue to use the current GPMS-based classifications.
- There is no direct correlation between the new classification policy and the old GPMS scheme. In general terms, policing assets that are classified up to and including **RESTRICTED** will be managed at **OFFICIAL** by partners, and assets marked at **OFFICIAL** that are received by forces will be managed at **RESTRICTED**.
- The impact analysis (as well as supporting the implementation work) activities will inform specific guidance to forces for the primary business processes.
- Specific attention is being paid to **CONFIDENTIAL** assets as they could be classified as either **OFFICIAL** or **SECRET** (based on the threats). **The National Crime Agency** have already done work in this area and general interim guidance will be based on their findings.
- Interim guidance will be available during March 2014.

Implementation

- The implementation of the classification policy will be designed to minimise the initial impact on policing. This includes:
  - Minimising the amount of ICT change required to implement the policy
  - Minimising the amount of training required for the scheme to be effective on day one.

- Implementation will be dependent on:
  - The SIRO for Policing accepting the overall risk, balanced against the business opportunities, for both the interim phase and post-implementation.
  - Chief Constables Council agreeing the impact analysis findings and transition plan.

- Once the scheme is implemented, it is envisaged that forces will use the point at which they change processes or technology to consider how the new policy can increase efficiency and effectiveness.

Critical Question

- How do we manage the diverse and varying range of sensitivities (with differing consequences resulting from the compromise or loss of information) within **OFFICIAL-SENSITIVE?**

- Cabinet Office guidance says:

> Individuals should be trained to exercise good judgement and provide meaningful guidance on how to handle any sensitive information that they originate, rather than relying on generic labels. However, in defined circumstances organisations may apply a DESCRIPTOR 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]’

- As part of the impact assessment, we will look at business processes and assess whether descriptors are required to manage the range of sensitivities within OFFICIAL-SENSITIVE. Where descriptors are required, these must be agreed nationally and may require partners (such as the CPS) to also agree them. Use of descriptors may also require changes to existing information sharing agreements.

Implications for National Systems

- Initially the impact on national police ICT systems should be minimal. The impact assessment will confirm this, but some minor changes may be required (to systems that print out documents with existing protective markings, for example).

- The contracts for many national systems come to an end in or around 2016. In preparation for this, the Home Office Police ICT Directorate is working with forces, PCCs, Cabinet Office and partners to develop a plan for national police ICT. The plan aims to:
  - Make the police IT that is delivered nationally more cost effective, and
  - Improve access for the police to data held on national systems that supports the fight against crime.

- As part of the plan, we will look at the wider implications of the move to the new classifications, and will seek to exploit the opportunities it opens up. This will include looking at consistent technical controls across systems.

- Systems that contain information currently considered CONFIDENTIAL will be reviewed as a matter of urgency, given the potential for some CONFIDENTIAL to become SECRET.

Next Steps

BRITISH TRANSPORT POLICE

A project team is being put in place. The next steps are to:

1. Establish a policing working group to develop and agree the interim guidance and implementation plan. This will include:
   - Forces – we have practitioners signed up but will also need business area representation.
   - CPS
   - HMCTS
   - Ministry of Justice
   - Home Office
   - Cabinet Office
   - NCA
   - College of Policing

2. Perform an analysis of current business processes, information assets and ICT systems to understand the impact of adopting the new policy.
   - We will take a risk-based approach, focusing on business processes where information passes from one organisation to another
   - CONFIDENTIAL information is also being looked at specifically.

Scope & Impact Assessment Approach

Scope

- All police forces in England, Wales and Scotland and Northern Ireland, including non-geographic forces and National Policing Systems.

Impact Assessment

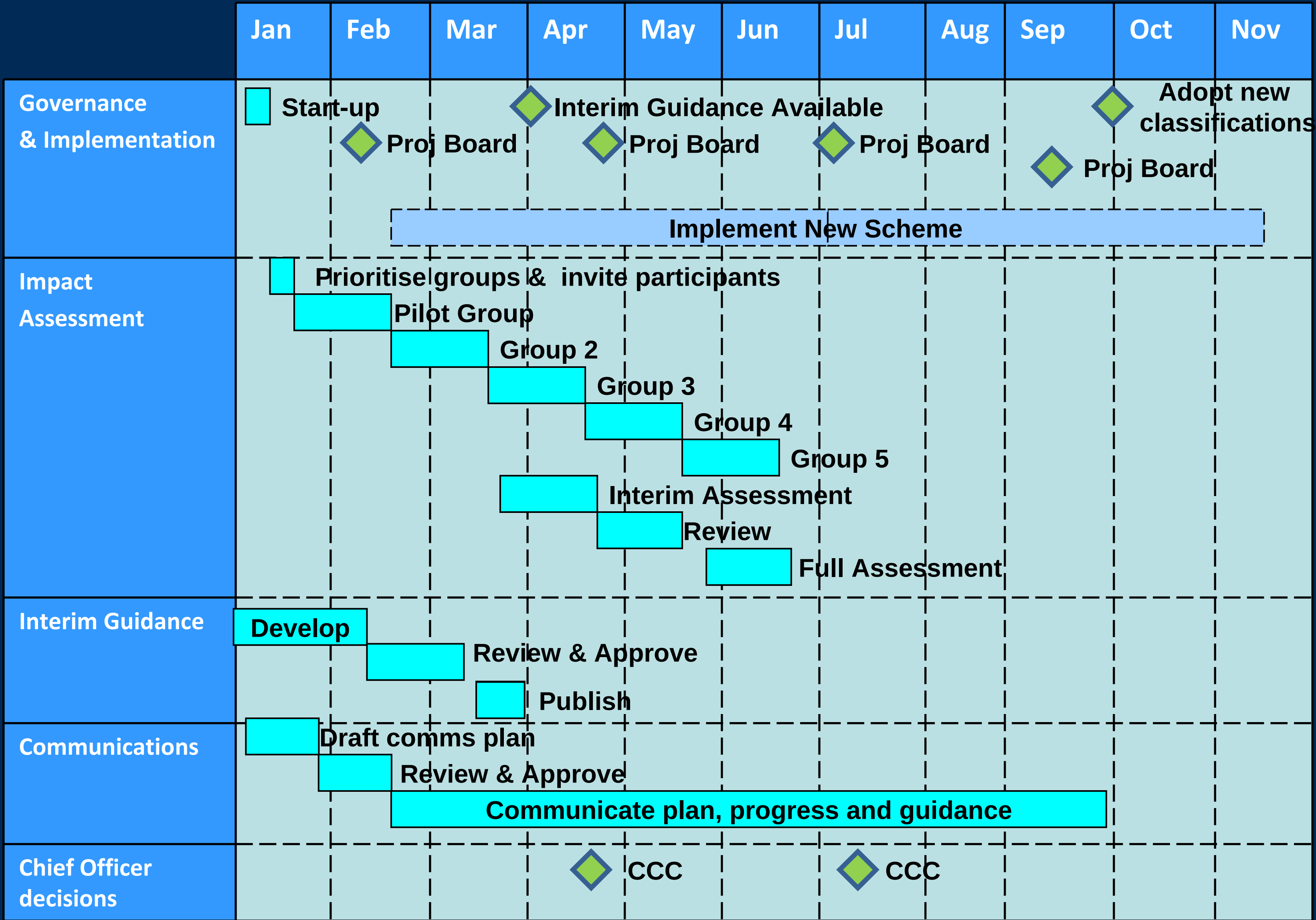
- The initial priority areas (to be agreed by the project board) for assessment are:
  - **Protecting Vulnerable People.**
  - **Incident and crime investigations.**
  - **Criminal Justice.**
  - **Collating and Managing Intelligence.**
  - **Managing People and Finances.**

- It will assess the level of change required to systems, processes and information. It will also assess the people and roles affected and, where possible, the work to make the changes.

- The analysis of each business group will involve workshops with the following representation:
  - **Police Force representatives.**
  - **College of Policing.**
  - **Business Process Owner.**
  - **Security Analyst.**

- The initial workshop will agree follow up actions which will be time-boxed to complete within 2-3 weeks of the workshop.

Outline Timeline



Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov

Governance & Implementation

- Start-up
- Proj Board
- Interim Guidance Available
- Proj Board
- Proj Board
- Proj Board
- Adopt new classifications
- Implement New Scheme

Impact Assessment

- Prioritise groups & invite participants
- Pilot Group
- Group 2
- Group 3
- Group 4
- Group 5
- Interim Assessment
- Review
- Full Assessment

Interim Guidance

- Develop
- Review & Approve
- Publish

Communications

- Draft comms plan
- Review & Approve
- Communicate plan, progress and guidance

Chief Officer decisions

- CCC
- CCC

Further Information

BRITISH TRANSPORT POLICE

- Further information on the GSC Policy can be found here: Classifications on gov.uk
- Information on the OFFICIAL classification, including an FAQ, can be found here: Managing Information Risk at OFFICIAL
- Contact: police.gsc@homeoffice.gsi.gov.uk.