Norfolk Police and Crime Commissioner (PCC) response to inspections of Norfolk Constabulary published by Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS)

Section 55 of the Police Act 1996 (as amended by section 37 of the Policing and Crime Act 2017) requires local policing bodies to respond to recommendations in inspectors reports within 56 days

Inspection Title:	Cyber: Keep the light on – An inspection of the police response to cyber-dependent crime
Date Published:	24th October 2019
Type of Inspection:	National Inspection

KEY FINDINGS:

In early 2019, the Home Secretary commissioned Her Majesty's Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) to inspect the effectiveness and efficiency of the police response to cyber-dependent crime by assessing whether:

- law enforcement has a well-designed strategy for tackling cyber-dependent crime;

- organisational structures provide the necessary capacity, capabilities and partnerships;

- victims of cyber-dependent crime receive a high-quality response; and

- staff at local and national levels are provided with appropriate learning opportunities to deal with cyber-dependent crime.

The inspection took place between April and June 2019 in ten police forces (Norfolk wasn't one of those inspected), in addition to three law enforcement agencies and nine regional organised crime units.

HMICFRS inspected how the police and the National Crime Agency deal with the threat presented by cyber-dependent crime and the wide range of criminals that commit it. This includes hostile state actors, organised crime groups, and those involved in online harassment. The subsequent report, Cyber: Keep the light on – An inspection of the police response to cyber-dependent crime, identified several areas of positive practice, including:

- efficient working arrangements between law enforcement agencies;

- a well-established national strategy for dealing with the threat from cyber-dependent crime;

- early identification and response to emerging threats;

- the implementation of minimum standards and recognised performance indicators; and

- the development of local cyber-dependent crime teams.

However, the Inspectorate warned that many of these achievements are undermined by inconsistencies in the response provided at a local level by forces. Specific issues included:

- concerns around the financial sustainability of capability and capacity at all levels;

- limited understanding of demand at a local level; and

- some forces not fully complying with initiatives to coordinate resources.

The report made one recommendation and four areas for improvement.

Recommendation

By 1 November 2020, the Home Office, the Cabinet Office, the National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime, the Director General of the National Crime Agency, and interested parties should revise the current police structure for the response to cyber-dependent crime. In doing so they should consider:

- the creation of a national police cyber-dependent crime network;

- the remit of any such network;

- how the network engages with other law enforcement agencies; and

- the tasking and co-ordinating responsibilities that will be required for the network to be effective.

Areas for improvement

There are some areas in which HMICFRS think those responsible for the police response to cyber-dependent crime and chief constables need to make improvements, but HMICFRS have not made specific recommendations about how those responsible should do this.

1. Chief constables should evaluate the use that their force makes of cyber specials and volunteers to ensure that they are used effectively.

2. With immediate effect, City of London Police should provide the Home Office with details of how the force intends to address the issue of reports being held in 'quarantine' within the Know Fraud system. Furthermore, the force should also identify its proposals to prevent a re-occurrence.

3. The National Police Chiefs' Council's lead for cyber crime and Coordinator for Economic Crime should revise the key performance indicators contained within the council's minimum capability standards for force cyber crime units. The revised standards should make clear:

- the minimum standards for investigation;

- the role of regional cyber crime co-ordinators in the recording, management, and review of cyber crime investigations; and

- the use of the weekly list provided by the National Fraud Intelligence Bureau to comply with the performance indicators.

4. The National Police Chiefs' Council Coordinator for Economic Crime should review the role the National Economic Crime Victim Care Units in providing advice and support to victims of cyber-dependent crime.

CHIEF CONSTABLE RESPONSE TO REPORT AND ANY RECOMMENDATIONS:

Norfolk Constabulary was not one of the forces inspected, however, the recommendation and areas for improvement are fully acknowledged.

In response to the increasing numbers of individuals and businesses becoming victims of cybercrime, a joint Cybercrime Unit was created in collaboration with Suffolk Constabulary in 2015. In addition to the joint unit, a Specialist Capability Team, temporarily funded by the Government's Police Transformation fund, has been established to operate until March 2020. The future funding of the Specialist Capability Team is under review, and work will continue to monitor and develop the Constabulary's response to cybercrime.

An area for improvement identified in the report is for forces to evaluate the use of cyber specials and volunteers to ensure that they are used effectively. In 2018, Norfolk and Suffolk Special Constabularies joined the "Cyber Specials and Cyber Volunteers scheme" (CSCV). In January this year, seven specials across Suffolk and Norfolk signed up and uploaded their biographies onto the National data base for Specials with specialist technical skills and experience. A Cyber volunteer has been recruited and is due to start with the Cybercrime team in January 2020. A further volunteer is looking to be recruited in the Spring 2020. The volunteers will be individually evaluated to determine their effectiveness.

PCC RESPONSE TO REPORT AND ANY RECOMMENDATIONS:

Throughout my four year term as Police and Crime Commissioner I have been committed to not only improving the effectiveness of policing in the county but to ensure that Norfolk Constabulary has the technology needed to keep our population safe in the face of the complex 21st century challenges it faces.

As PCC with responsibility for the victim I am all too aware of the impact cybercrime can have on its victims both in terms of distress and harm, and inconvenience. I am assured, as is evidenced by its proactive work in this area to date, that Norfolk is a force which takes cybercrime seriously and is committed to continuing to tackle this evolving threat. That said, while it is pleasing to see the progress that has been made to date, we must always be mindful that cybercrime is an ever present and ever-changing threat, and so cannot rely on past achievements to deliver future protection.

While Norfolk Constabulary was not one of those inspected, I note the recommendations and, through my office's existing accountability framework will continue to monitor progress and development in this area.

For Office Use Only:

- ✓ Response forwarded to HMICFRS Section 55 Responses
- ✓ Response forwarded to Chief Constable
- ✓ Response forwarded to Police and Crime Panel
- ✓ Response published on the OPCCN website