OFFICIAL REPORT
AITHISG OIFIGEIL

DRAFT

Economy and Fair Work Committee

Wednesday 4 March 2026

The Scottish Parliament
Pàrlamaid na h-Alba

Session 6

Wednesday 4 March 2026

CONTENTS

ECONOMY AND FAIR WORK COMMITTEE
7th Meeting 2026, Session 6

CONVENER

Daniel Johnson (Edinburgh Southern) (Lab)

DEPUTY CONVENER

*Michelle Thomson (Falkirk East) (SNP)

COMMITTEE MEMBERS

*Sarah Boyack (Lothian) (Lab)
*Willie Coffey (Kilmarnock and Irvine Valley) (SNP)
*Murdo Fraser (Mid Scotland and Fife) (Con)
*Stephen Kerr (Central Scotland) (Con)
*Gordon MacDonald (Edinburgh Pentlands) (SNP)
Lorna Slater (Lothian) (Green)
*Kevin Stewart (Aberdeen Central) (SNP)

*attended

THE FOLLOWING ALSO PARTICIPATED:

Paul Chapman (Scottish Government)
Angela Constance (Cabinet Secretary for Justice and Home Affairs)

CLERK TO THE COMMITTEE

Anne Peat

LOCATION

The James Clerk Maxwell Room (CR4)

Scottish Parliament

Economy and Fair Work Committee

Wednesday 4 March 2026

[The Deputy Convener opened the meeting at 09:00]

Decision on Taking Business in Private

The Deputy Convener (Michelle Thomson): Good morning and welcome to the seventh meeting in 2026 of the Economy and Fair Work Committee. I will chair today’s meeting, because our convener, Daniel Johnson, has given his apologies. Lorna Slater has also given apologies.

Our first agenda item is consideration of whether to take items 3 and 4 in private. Are members agreed to take those items in private?

Members *indicated agreement*.

Cyber Security and Resilience (Network and Information Systems) Bill (UK Parliament Legislation)

09:00

The Deputy Convener: Under agenda item 2, I welcome to the meeting the Cabinet Secretary for Justice and Home Affairs, Angela Constance. She is accompanied by Scottish Government official Paul Chapman, who is head of public sector cyber resilience.

I understand that you would like to make a short opening statement, cabinet secretary.

The Cabinet Secretary for Justice and Home Affairs (Angela Constance): Good morning. I think that this is the first time that I have been to the Economy and Fair Work Committee as justice secretary. However, in a previous session, in the dim and distant past, I served for a wee while on this committee—I think with Willie Coffey at some point.

I am pleased to be here to discuss the legislative consent memorandum, which will enable several clauses of the Cyber Security and Resilience (Network and Information Systems) Bill to take effect in Scotland. Cyberthreats are growing in scale and sophistication, and they pose a real threat and risk to essential services that people, communities and businesses rely on every day. As systems become more digitally interconnected, the impact of any single incident can spread very quickly. We must therefore make sure that our laws and regulations keep pace with the change in risk and the evolving challenge.

The bill strengthens and updates the existing network and information systems regulations and expands the scope to include digital and operational services, such as managed service providers, large data centres, large load controllers and designated critical suppliers, all of which play a major role in the delivery of essential national activities. The bill also strengthens the powers of competent authorities in key areas, including information gathering, incident reporting, cost recovery and enforcement.

In addition, the bill provides the United Kingdom Government with the tools to ensure a consistent strategic direction for the UK. That includes powers for the secretary of state to publish strategic priorities, issue a code of practice for regulators and direct operators of essential services and competent authorities where there are national security concerns. For those measures to be effective, they must be applied consistently across all four nations. Many operators, regulators and suppliers work across national borders, and fragmented arrangements could create avoidable burdens that would weaken our collective resilience. A co-ordinated approach is strongly supported by stakeholders, and it also aligns with the ambitions that we set out in the updated strategic framework for a cyber resilient Scotland, which I launched in November last year.

The Scottish Government therefore proposes legislative consent for clauses related to critical suppliers, incident reporting, cost recovery, information gathering, information sharing, content of guidance, financial penalties, enforcement, appeals, code of practice, progress reporting and inspections. Those changes will give competent authorities, including Scottish ministers and the Drinking Water Quality Regulator for Scotland, enhanced powers to ensure cybersecurity and resilience across devolved sectors. Expanding the scope to include managed service providers and critical suppliers reflects the reality of complex supply chains and the potential impact of cyber incidents across sectors. It also directly supports the ambitions in our strategic framework.

However, parts of the bill are still subject to on-going discussions with the UK Government. Those include provisions where current drafting lacks explicit requirements to consult or seek consent before altering Scottish ministers’ executive competence or before amending acts of the Scottish Parliament through secondary UK legislation. Those matters are likely to form the basis of a supplementary legislative consent motion in the coming months, as the bill progresses.

Cybersecurity and resilience are shared responsibilities. The bill offers important and timely improvements to the UK’s cyber regulatory framework, and we support measures that strengthen our ability to protect critical services in Scotland.

The Deputy Convener: Thank you, cabinet secretary. I will open with the first question.

You have set out some of the context. It appeared to me, in preparing for this evidence session, that the Scottish Government has not yet recommended consent in relation to a number of clauses and that how the bill would operate in practice—where, in effect, it would grant additional power to the Scottish Government—has to be considered in further detail. There is also the issue of the clauses that would give the secretary of state power to take action without consent from the Scottish Government. Am I correct about those two areas? Will you give us a little more flavour in relation to where the discussions on those two different areas are at?

Angela Constance: Before I get into the specifics of that, I will give some context in order to underline the importance of the work that we are doing with the UK Government on what is a reserved matter that impacts devolved services.

The National Cyber Security Centre noted in its annual review, last October, that it had dealt with 204 nationally significant cyberattacks against the UK in the 12 months to August 2025. That was a sharp rise from 89 in the previous year. It is important that we bear in mind the context of that increasing threat, which is becoming increasingly sophisticated. That is the fundamental and core focus.

We support many of the amendments, particularly around the update to the Network and Information Systems Regulations 2018. Most of the discussions that we are having are, as the deputy convener identified, with reference to the powers conferred on the secretary of state—in essence, clauses 25 to 41.

Although, as a point of principle, we broadly support the additional powers conferred on the secretary of state, we have concerns, which are subject to further dialogue, about where those powers have the potential to alter the executive competence of the Scottish Government or to amend acts of the Scottish Parliament through secondary legislation without the explicit need to consult or seek the consent of Scottish ministers.

We always take a pragmatic view on such things, particularly about what will work in practice when the legislation is implemented. There is a very good relationship between my officials and the Department for Science, Innovation and Technology—they work well together. However, it is fair to say that there is a difference of view on some of the amendments.

In this area of the bill, we are giving consent to only one clause—clause 38—and withholding consent on the rest at this time, in order to allow for further discussions. The discussions tend to proceed quite slowly. In my experience, they are rarely done rapidly, and there are all sorts of reasons for that.

At the start of February, the UK Government gave us its view that it did not think that any further drafting or amendment of the clauses was required. Scottish Government officials, including from the legal directorate, have compiled a view. We wrote to the UK Government last month, and we are still waiting for a response.

The Deputy Convener: I know that you might not want to be drawn on this, but what are your predictions of how this might pan out? In your framing, you have made it clear that the increasing incidence of cyberattacks is linked to geopolitics.

However, the executive competence consideration is fundamental to this.

Angela Constance: It is difficult to answer that question without going through the bill clause by clause. As I said, we are still in negotiations, and I want to be respectful of that. I do not want to be obtuse with the committee, but I also do not want to show my hand.

I suppose that any final Scottish Government position or recommendation to the Scottish Parliament will depend on our view of the bill clause by clause. Where we have a more fundamental concern is around the ability of UK secondary legislation to alter Scottish primary legislation. That is a fundamental concern—it is my central concern in all this.

In my experience of dealing with other pieces of legislation, as well as focusing on principles, it is very often about how the legislation would work in practice. However, as I said, there is a fundamental issue here, bearing in mind that we do not know what a future UK Government or a future Scottish Government will look like. It is all very well to say that, in this instance, relationships are positive and constructive, but the notion of UK secondary legislation—very quickly, with a lower level of scrutiny—

The Deputy Convener: A lack of scrutiny.

Angela Constance: —changing our primary legislation is fundamentally concerning. I would hope that we are in consensus about that, at least in this Parliament.

The Deputy Convener: I think that that is clearly understood.

My follow-on question is on timescales. I know that there has been a carry-over motion in Westminster. Set against the backdrop of urgency—the legislation being required due to the increase in incidents and our inevitably going into dissolution and an election campaign—what is your thinking on, or what discussions have been had and arrangements made with the UK Government about, the urgency with which this will be taken forward once the new session of the Scottish Parliament gets under way?

Angela Constance: Any future LCM will fall to the next session of Parliament. By way of some reassurance, ministerial work does not stop during purdah. There are significant constraints on making major or impactful decisions, and you will not see substantial announcements or things like that, but some work continues, particularly at official level.

On the UK Government's timetable for the bill, right now, it does not anticipate royal assent until early 2027, with the bill being fully in force in late 2028.

At the start of February 2026, the bill went to committee stage in the House of Commons, and in late summer and early autumn this year, the Department for Science, Innovation and Technology intends to consult on implementing policy. There will then be further consultation on strategic priorities. There is still a journey to go on with the bill, important as it is.

09:15

The Deputy Convener: We have a supplementary question from Mr Stewart.

Kevin Stewart (Aberdeen Central) (SNP): Good morning, cabinet secretary. There is quite a long timescale for the bill. Earlier, I was relating to committee members a question that I was asked by a schoolboy from Robert Gordon's College in Aberdeen. He was asking about legislating for information technology, artificial intelligence and cybersecurity, and he said that legislation and regulation take far too long. You have already covered what is a pretty lengthy timescale.

This all started in 2022, I believe, from initial conversations in 2018. Cabinet secretary, I recognise that you want to protect the Scottish Parliament as much as possible—as you always do—and our primary legislation in particular. You have concerns here, and I do, too. In some regards, are we going to have to find a way under the devolved settlement, with partners—or even if we were an independent nation—to change, globally, how we frame legislation when it comes to such issues? The baddies—to put it frankly—are able to move very quickly in what they are doing, yet we seem to take forever to legislate and regulate.

Angela Constance: The point about the criminal world and the changing nature of crime and offending is that things are moving at pace. As was indicated earlier, the threat is increasing and is becoming more sophisticated.

The timescale for the bill is not within my gift. It is fair to say that there are probably other examples of both the Scottish Government and the UK Government having legislated at pace. I have been involved with some of that legislation. I am thinking about the Post Office legislation—the quashing of convictions would be an example of things having operated at pace.

On the point about global connections and the global aspect of crime, geopolitics plays into that, of course. One positive about the bill from the UK Government is that it aligns more with the European Union's network and information security directive 2—the NIS2 directive—and the

EU's Cyber Resilience Act has implications for the UK. It is not that we are subject to that legislation, but many businesses operate internationally, so they are already complying with it.

Just to be clear, the Network and Information Systems Regulations 2018 and the bill clearly cover a reserved area, but there are devolved aspects around the regulation of sectors such as health, drinking water, roads, cross-border rail services and onshore oil and gas.

The Deputy Convener: Gordon MacDonald also has a supplementary.

Gordon MacDonald (Edinburgh Pentlands) (SNP): Good morning. As you quite rightly said, cabinet secretary, the bill will not come fully into force until 2028, so I am keen to understand what we can do in the short term. We have had a number of cybersecurity breaches—Western Isles Council in 2023, and West Lothian Council and Glasgow City Council in 2025—and reports into those incidents suggest that they were partly due to overdue information technology health checks, a lapse in public service network certifications and untested incident response plans.

Given that these attacks happen regularly and that the bill will not come fully into force until 2028, what can we do in the short term to make sure that Scottish public services are looking after the nuts and bolts of the system before they have to worry about ransomware?

Angela Constance: The Scottish Government and our partners use the strategic framework for a cyber resilient Scotland, which was launched in 2021. It was published in the aftermath of and in response to the Covid-19 pandemic, which changed our view and forced modernisation in some areas, particularly in relation to the use of technology and its role in public services and public safety. At the end of last year, the framework was updated. We cannot change the law, but the purpose of the framework is to ram home the fact that there are cyber risks that need to be recognised and managed across the public, private and third sectors.

Scotland has a flourishing cybersecurity industry, including a research community and a skilled cybersecurity workforce, so we need to galvanise that. On the nuts and bolts, the CyberScotland partnership brings together cross-sectoral partners, and the national cyber resilience advisory board gives advice and direction to Scottish ministers and the Scottish Government. The Scottish cyber co-ordination centre provides the central co-ordination function for improved intelligence sharing and early warnings, and national incident co-ordination for the public sector in Scotland. The centre is principally led and supported by the Scottish Government, but it has a secondee from Police Scotland. It is about being able to give information that contributes to intelligence and the management of threat. Police Scotland has also recently set up its cyber and fraud unit.

The Deputy Convener: Before I bring in the next colleague, I want to ask one more question. Not that long ago, I was out with the Finance and Public Administration Committee in Lithuania, which runs its entire estate off client-server architecture. It has thousands upon thousands of cyberattacks. Given the sophistication of how it runs its estate and the volume of cyberattacks that it has, has anybody from the Scottish Government reached out to Lithuania to ask about best practice? Lithuania's geographic location probably indicates why it has had such an increase in attacks, but it might be worth while considering that approach.

Angela Constance: I have not been to Lithuania, just for the record, but I do not know whether Mr Chapman or any of his colleagues have been there.

Paul Chapman (Scottish Government): We have spoken to a number of countries across Europe at various levels about the differences in their architecture and how they have done it. A lot of them have advantages in that they started from almost nothing and had to build it. The rest of us are having to catch up and retrofit things into what we already have. We have a huge amount of legacy across the sector, but we are indeed talking to international partners, in Europe and beyond.

The Deputy Convener: Thank you.

Murdo Fraser (Mid Scotland and Fife) (Con): Good morning, cabinet secretary. I want to move on to some slightly more practical issues with regard to the legislation. I appreciate this is not a Scottish Government bill but a UK Government bill, but it will have an impact on Scotland. Given what you have said, I assume that the Scottish Government is, generally speaking, supportive of the direction of travel and recognises the need for the bill, but it will come at a cost not only to business, and particularly suppliers to the private sector in fields such as IT, but to the public sector—for example, the national health service. Has the Scottish Government done any assessment of the likely cost either to business and the private sector or to the public sector?

Angela Constance: Broadly speaking, yes. As the bill updates existing regulations, it is not expected that there will be any immense or unwieldy costs. We are continuing to monitor and look at that, though, because things can change as a result of some quite small detail in an amendment, and we have to be alert to that.

We are conscious of the impact on small to medium-sized enterprises, and we will work with the UK Government in and around that area. Mr Chapman will keep me right if I do not get this right, but competent authorities will be able to designate those providing services that are essential and absolutely crucial to the country. Although such authorities would see that as a last resort, given the additional burden on SMEs, we have to be alert to that. I ask Paul Chapman to say a bit more about the practicalities.

Paul Chapman: The bill gives the power to designate critical suppliers, but designation is very much seen as a last resort by most of the competent authorities that are out there at the moment. That is part of the consultation on implementation that was noted earlier so that we can try to work out how it will work in practice. However, at the moment, it is more likely that, instead of going down the designation route, a competent authority would encourage its operator of essential services to manage its supply chains appropriately through the levers that it already has. As I said, designation is likely to be a last resort in order to deal with any problems or, indeed, any potential concentration risk. Where there are common suppliers providing vital services across different sectors, we might want to look at them differently. Outside of that, though, we would not expect those bodies to have more of a burden placed on them, other than the contractual arrangements that they already have with operators of essential services.

Murdo Fraser: The bill suggests that the cost will be £12 million across the UK, and it might be assumed that Scotland will bear a proportionate share of that across the public sector. However, you do not expect that to be a major burden.

Angela Constance: Not just now. I point out that SMEs are currently below the threshold for registration as operators of essential services. That said, we will be cognisant of any changes that are made. There is a bit of a road for the bill to travel, and we need to be alert to that.

Murdo Fraser: Thank you.

The Deputy Convener: Stephen Kerr has a supplementary.

Stephen Kerr (Central Scotland) (Con): I just wanted to ask Paul Chapman about the expected number of critical suppliers, given the criteria that he has set out.

Paul Chapman: It will be vastly different across the UK and will depend on the sectors in which they are designated. Some of the larger sectors—for example, the more reserved sectors such as energy—might well look to designate critical suppliers.

Stephen Kerr: What about health?

Paul Chapman: Health is devolved, so I think that any impact will be very unlikely. At the moment, the competent authorities for the health sector are, obviously, governing public bodies. A lot of the measures in the NIS regulations do not make a lot of sense when applied to a public body. Things such as penalties and fees are not applied to the health sector as such by the competent authorities because it does not make a lot of sense to charge them a penalty.

09:30

Stephen Kerr: What is your assessment of public bodies' financial exposure to penalties, which are quite severe and are aligned with the existing data protection fines of up to £17 million?

Paul Chapman: For public bodies, it would be very little. Again, that would be an act of last resort. There are about 23 operators of essential services across NHS boards in Scotland and Scottish Water, and the competent authorities are fully devolved. It makes no sense to apply those penalties to them. That money would be taken out of the system when it could be used far more usefully to secure the estates of those operators of essential services.

Stephen Kerr: What about the reporting requirements? They are quite onerous. I suppose that it depends, because you have narrowed the scope of who might be subject to them, but for public authorities in a crisis, the 24-hour and 72-hour reporting requirements are still quite onerous.

Angela Constance: That is the initial reporting, and then there would have to be follow-up reporting. There will be a new duty under the bill when it is enacted, but speed is of the essence, given our reliance on public services. We have to be able to get information quickly, so that Police Scotland or the Scottish cyber co-ordination centre can get information out to other bodies that might be impacted.

Stephen Kerr: Are you quite confident that the health boards or any of those designated critical suppliers in the supply chain can realistically comply with the 24-hour and 72-hour reporting requirements?

Angela Constance: That would be my view, Mr Kerr, and it is imperative that people comply with the requirements, given the nature of the threat.

Stephen Kerr: Okay—that is fair enough.

The Deputy Convener: Do you want to ask any more questions?

Stephen Kerr: No. I think that some of my other points were covered earlier, particularly on clause

41 and the Henry VIII powers. I am pretty satisfied with what I have heard.

The Deputy Convener: I just want to pick up on bottoming out on costs. Our primary interest today is the LCM, but there are going to be general increased costs to businesses as a result of the need to be uber-alert to cyber threats. Do you think that the bill and the way that any new Scottish Government treats it will emphasise the need for all levels of business to be aware of such threats? I am not entirely sure that there is the level of awareness that there needs to be from a purely economic perspective.

Angela Constance: I am not surprised that the convener of the Economy and Fair Work Committee is asking that question. It is clear to me, as justice secretary, that cybercrime is a threat not only to our national security but to our economy. We are going to have to consider the risk profile of threats to Scotland and the UK as a whole and in the round. My focus is obviously on national security, although it is reserved, and combatting crime. Crime is used for economic advantage, and that has a huge cost to taxpayers and business.

There is also the issue of how businesses are supported to upskill and uptool, and I contend that that has to be a cross-Government consideration.

The Deputy Convener: Sarah, do you want to come in?

Sarah Boyack (Lothian) (Lab): Thank you, convener. My question follows on perfectly from the point that the cabinet secretary has just made about the costs. Our briefing says that cyberattacks cost the UK £15 billion every year. I presume that there is also a significant cost for Scotland, so it would be useful if she could put that on the record.

We have spoken briefly about the NHS. To make this all real, can the cabinet secretary give us some examples of the designated competent authorities and the regulatory authorities that will be covered by the legislation in Scotland?

Angela Constance: I will begin, before handing over to Mr Chapman.

Ms Boyack makes a good point about the cost of doing nothing. There is a cost to the crime and the threat and therefore a cost to doing nothing, which must also be considered.

The Scottish Government is the competent authority for health services and the Scottish Water regulatory body is the competent authority for the water sector. We came to an agreement about cross-border rail, but that was before my time.

Paul Chapman: It is the Department for Transport.

Angela Constance: We came to agreement on that.

I will hand over to Mr Chapman.

Paul Chapman: Some other elements are partially devolved. The authority for roads is partially devolved but there are no operators that meet the criteria. Onshore oil and gas are also devolved, but, once again, nothing meets the criteria for an operator of essential services in those areas.

Effectively, the only active competent authorities dealing with aspects devolved to Scotland are the Drinking Water Quality Regulator for Scotland and—with regard to the health sector—Scottish ministers. All other areas are reserved to the UK, including energy, which is regulated by the Office of Gas and Electricity Markets, and transport, which is covered by the DFT.

Sarah Boyack: That is helpful. Those are the regulatory authorities, but there might be an issue with the businesses that supply services. To pick up on Murdo Fraser’s comments, there is also an issue with SMEs. We got a briefing from the Association of British Insurers about the costs and benefits of tackling that. How do you communicate with a vast range of organisations to ensure that they are up to speed? There is a reference in our papers to a round table, and the cabinet secretary also mentioned a workforce partnership, a resilience body and a co-ordinating centre. How does information and knowledge get communicated from the centre to the raft of organisations that will have to change how they operate?

Angela Constance: I spoke about the core purpose of the strategic framework for a cyber resilient Scotland, which tries to look at the whole system and the whole country, including the public sector, industry and the third sector. We must go deeper and further and that will be a crucial part of the work of economy ministers and others, such as health ministers, who need to be in that terrain.

Paul Chapman: The other thing to mention is the CyberScotland partnership, which provides a one-stop shop through an online portal that is available to all. That partnership includes a number of organisations that reach out across the private sector, including SMEs, through things such as Business Gateway.

Last week was the annual CyberScotland week. Events under that banner run all across the country every year to promote cybersecurity and resilience to the public, private and third sectors, in support of the action plans under the strategic framework for a cyber resilient Scotland.

Willie Coffey (Kilmarnock and Irvine Valley) (SNP): Cabinet secretary, I would like to hear your views on how we are working with the European Union on the issue. You mentioned the NIS2 directive. How harmonious are arrangements in the UK, in comparison with those in the European Union?

Angela Constance: The same logic behind having a common approach across the UK—bearing in mind that, geographically, we are an island and businesses operate across geographical boundaries—applies to the European context as well. It is a stated aim of this Government that we want to maintain alignment with the EU, and we believe that that is in the interests of business.

There are businesses in Scotland and the UK that operate across the UK and in Europe. Because they operate in Europe, those businesses need to comply with the NIS2 directive and the EU's Cyber Resilience Act. That partly helps to alleviate the concerns that were expressed earlier about additional burdens and costs, because there are many businesses that are already operating to a particular standard.

Willie Coffey: As we all know, cyberattacks can be carried out by individuals—for example, by students in bedrooms—but they can also be carried out by orchestrated non-UK agents, and they can be directed at any target whatsoever. That takes us to the more defensive side of cybersecurity and national security. Do you know of any work that is going on between the UK Government and the European Union to further strengthen and integrate national defensive cybersecurity arrangements and to assess the risks of having separate approaches to cybersecurity as a result of the UK leaving the European Union? Is there an attempt to try to integrate such defensive measures more consistently across the European Union and the UK?

Angela Constance: I will start broadly from a fairly narrow justice perspective, and then Paul Chapman can add more detail if he wishes.

With our removal, against our will, from the European Union, well-oiled information-sharing arrangements such as the European arrest warrant and various systems of sharing intelligence, which had evolved over the decades and were operating smoothly and well, were disrupted. It took some time, post-Brexit, to find workarounds and alternative arrangements. There are now alternative work arrangements. Law enforcement agencies tell me that those are more bureaucratic, but different systems are now in place.

I do not know whether Mr Chapman has any other information on the detail of engagement between the UK and Europe regarding cyber resilience.

Paul Chapman: I can add a bit of detail. The National Cyber Security Centre, which is the UK's technical authority on cyber, maintains links across Europe. We are well plugged in on the threat and intelligence side of things.

The NIS2 directive is a bit wider and went a bit further than the provisions that are in the Cyber Security and Resilience (Network and Information Systems) Bill at the moment. The point of the bill is to lay the groundwork for more speedy future changes, so that we can react to the changing situation. The link across to Europe is vital in understanding what those needs might be. We link into that through the structure—

Willie Coffey: So, there is a dialogue.

Paul Chapman: Yes, there is definitely a dialogue.

Willie Coffey: Thank you.

09:45

The Deputy Convener: The evidence session has deliberately been allowed to drift into areas of general concern about cybersecurity rather than focusing on just the LCM—I ask the cabinet secretary to indulge us on that, given that we are the Economy and Fair Work Committee.

I have a final question. How is cyber generally being managed in the Government? Is it your directorate that, by reacting to criminal situations, is leading on cyber and feeding that through to other directorates? Cyber has potential impacts for every cabinet secretary and minister, and they should all be alive to that.

It would be helpful to understand how the approach is working at a high level, which may be something that a future iteration of this committee wants to follow up.

Angela Constance: It depends on the incident. There is directorate support, but the point about leadership depends on whether the incident involves, for example, a local authority, a school or a health board. There may be particular portfolios and ministers that are more impacted at particular times and that are pushed for a response—

The Deputy Convener: But that is a reactive response rather than being proactive, which is the point that I am getting at.

Angela Constance: Indeed. The digital directorate in the Scottish Government is core and fundamental to all this. However, if the committee would like me to pursue further information with other ministers, I would be delighted to do so.

The Deputy Convener: That is very useful.

Thank you for your attendance today. That concludes questions from the committee, unless either of you wants to add any final comments.

Angela Constance: No.

The Deputy Convener: Thank you. That concludes the public part of the meeting.

09:46

Meeting continued in private until 10:14.

Official Report
Room T2.20
Scottish Parliament
Edinburgh
EH99 1SP

Email: official.report@parliament.scot
Telephone: 0131 348 5447

Published in Edinburgh by the Scottish Parliamentary Corporate Body, the Scottish Parliament, Edinburgh, EH99 1SP

All documents are available on
the Scottish Parliament website at:

www.parliament.scot

Information on non-endorsed print suppliers
is available here:

www.parliament.scot/documents

For information on the Scottish Parliament contact
Public Information on:

Telephone: 0131 348 5000
Textphone: 0800 092 7100
Email: sp.info@parliament.scot

The Scottish Parliament
Pàrlamaid na h-Alba