



Data Standards Authority : Vulnerability Working Group Meeting Summary

Attendees

<p>Firoze Salim - CDDO Didac Fabregas-Badosa - CDDO Paul Davidson - iStandUK (Tameside MBC) Shelley Heckman - iNetwork (Tameside MBC) Murat Soncul - CDDO Suzanne Fry - CDDO Mohammed Waqas - CDDO Elliot Robinson - HMRC Jack Roberts - Social Finance* James Elliot - HMT Kate Cooper - LGA Malcolm Davies - HMT Matthew Roberts - DLUHC Mike Thacker - Porism Nicholas Oughtibridge - NHS Oliver Southwick - Social Finance* Shantanu Guha - DWP Simon Roberts - Improvement Service Samuel Thomas - MoJ Jasmine Wilson - MoJ Kirsty Hendry - DLUHC Connor Malone - DWP</p> <p>*Standing for DfE Data</p>	<p>Apologies: Rachel Davison - DWP Carla Taylor - MoJ Claire Bell - ONS</p>
---	---

Record of discussions

1	<p>Welcome, introductions and agenda Didac Fabregas-Badosa, CDDO</p>
	<ul style="list-style-type: none"> ● Didac welcomed attendees and asked the new working group members to provide a quick introductory statement for the benefit of the meeting.
2	<p>“Where are we?” Didac Fabregas-Badosa, CDDO</p>
	<ul style="list-style-type: none"> ● Didac provided an overview of the work that CDDO and SAVVI have done to date. This includes: <ul style="list-style-type: none"> ○ Engagement with a wide range of stakeholders and expansion of the membership base for the working group ○ Extensive desk research in the vulnerability space ○ Update the ToR based on the discussion and comments from the first meeting ○ Development of three product specifications based on the opportunities identified by the WG during the first meeting. The product specifications have been grouped in three main categories: Modelling, Terminology and Enabling. To note that the product specifications were shared ahead of the meeting with the group. <ul style="list-style-type: none"> ■ Didac explained that the delivery of the product specifications requires sequencing as the modelling product sets the conceptual basis for the other two product workstreams.
3	<p>Product Specification 1 - Modelling Didac Fabregas-Badosa, CDDO Paul Davidson, iStandUK (Tameside MBC)</p>
	<ul style="list-style-type: none"> ● Didac briefly presented the first product specification: Modelling, which consists of three potential deliverables: <ul style="list-style-type: none"> ○ A common definition of vulnerability. Each department has its own definition of vulnerability, which tends to be focused on the organisation's remit and services. A single definition of vulnerability would be inclusive of existing departmental definitions and could be applied across a wide range of vulnerability scenarios. ○ A concept model for vulnerability. As a foundation for setting data and process standards, a concept model would map out the domain of “vulnerability” ○ A logical model for vulnerability. As a foundation for proposing interoperability standards, a logical model would set out data structures that can share vulnerability data. ● Paul Davidson provided illustrated examples on how the deliverables could look like (full examples available in the slides). For example:

	<ul style="list-style-type: none"> ○ A common definition of vulnerability: Paul shared that SAVVI defines vulnerability as “An Increased Risk of a Poor Outcome”, which is broad enough that allows capturing a wide range of vulnerabilities
	<p>Discussion</p> <ul style="list-style-type: none"> ● Oliver Southwick highlighted that it may be challenging to find and agree on a common definition of vulnerability as organisations tend to have their own. He suggested that the key for success is to have a wide range of stakeholders involved in the process to craft a wide and inclusive definition. ● Nicholas Oughtibridge pointed out that the baseline idea of vulnerability could be “risk of harm”. He noted that a definition of vulnerability based on a risk-approach could be an option to consider for the working group. He argued that following this approach a wide and broad ranging definition of vulnerability could be produced and would not lead to any disagreements. ● Didac asked the members to share any definitions of vulnerability currently used within their organisations. ● No objections were raised on the approach taken.
<p>4</p>	<p>Product Specification 2 - Terminology Didac Fabregas-Badosa, CDDO Paul Davidson, iStandUK (Tameside MBC)</p>
	<ul style="list-style-type: none"> ● Didac briefly presented the second product specification: Terminology, which consists of two potential deliverables: <ul style="list-style-type: none"> ○ Exploration of vulnerability scenarios. After the working group discussed some vulnerabilities such as becoming homeless, coping during flood and managing debt, this deliverable would look at selecting one or more vulnerability scenarios and developing a narrative to explain how data is or could be shared to find and support vulnerable people. ○ Taxonomies for vulnerabilities. A common understanding is essential and for standards to be scalable and reusable, it is proposed that hard-coded fields and definitions should be avoided, and replaced with links to agreed definitions. The proposed deliverable would look at selecting concepts from the concept model that could potentially become the class of a taxonomy and could be grouped in a list that would support a vulnerability scenario. ● Paul Davidson provided illustrated examples on how the deliverables could look like (full examples available in the slides). For example: <ul style="list-style-type: none"> ○ Exploration of vulnerability scenarios: Paul presented detail on the “flooding” vulnerability scenario, providing clear examples of the purpose, needs/outcomes, risk model(s) and data to be potentially reused to respond to such vulnerability.
	<p>Discussion</p> <ul style="list-style-type: none"> ● Suzanne Fry indicated that this work could and should potentially build from already existing taxonomies, and that considering those as departure points it is

	<p>essential. Suzanne suggested narrowing down the taxonomies work based on particular outcomes or vulnerabilities rather than trying to cover “too much”.</p> <ul style="list-style-type: none"> ● Paul Davidson stressed the importance of reusing existing work and building from it. Paul raised the point that the LGA has done some work in this space. ● Nicholas Oughtibridge echoed Suzanne and Paul’s point about building from existing work. On particular indicators for vulnerabilities, Nicholas highlighted the importance of differentiating between characteristics and circumstances, as both are valuable but are different indicators. ● Simon Roberts provided a real life example: the ongoing work in Scotland around trying to bring down the levels of drug harm. Simon explained that a data advisory group is working in the space and briefly explained the operations and mechanism in place. ● No objections were raised on the approach taken.
<p>5</p>	<p>Product Specification 3 - Enabling Didac Fabregas-Badosa, CDDO Paul Davidson, iStandUK (Tameside MBC)</p>
	<ul style="list-style-type: none"> ● Didac briefly presented the third product specification: Enabling, which consists of two potential deliverables: <ul style="list-style-type: none"> ○ Information Governance (IG) Framework. An IG framework to set out the steps to take in order to share data for a vulnerability initiative. Lots of guidance already exists that includes the reuse of existing data to support a vulnerability initiative. However, departments are likely to have their own IG frameworks that focus on supporting their own services. ○ Supporting guidance relating to data security, service considerations and data matching. Standards are only one of the considerations to get right for a multi-agency vulnerability initiative to succeed. <ul style="list-style-type: none"> ■ Didac raised that this work will look at building from already existing resources in place developed by central government departments, local government, government agencies and regulators. Didac stressed that this work does not aim to replace any of the existing resources but to build from those and make sure that these are relevant and applicable to different vulnerability scenarios. ● Paul Davidson provided illustrated examples on how the deliverables could look like. For example: <ul style="list-style-type: none"> ○ Data security, service considerations and data matching. Paul shared the example of the Greater Manchester Distributed Data Mesh, which illustrates a wide GMCA network but with different nodes that make “cuts of data” from operational data sets available. This allows for the minimal data sharing to provide specific services or achieve particular goals while securing other data assets that are not relevant for purpose.
	<p>Discussion</p>

	<ul style="list-style-type: none"> • Nicholas Oughtibridge flagged that this is one of the most crucial deliverables for the working group to succeed and achieve change. However, he recognised that this is one of the most resource intensive deliverables. Nicholas suggested that the group could and should also look at different behavioural standards in terms of information governance. • Kate Cooper showed support for the product specifications. Kate also asked how CDDO/SAVVI is planning to gain support from different stakeholders to adopt and roll out the agreed actions and resources. <ul style="list-style-type: none"> ○ Firoze Salim explained that the vulnerabilities working group has been established under the umbrella of the Data Standards Authority. Firoze shared that the DSA works collaboratively across government to ensure that its outcomes capture a wide range of views. Firoze also reminded the attendees that the DSA can encourage and/or mandate standards for cross-government adoption. • Oliver Southwick pointed out that an IG Framework would be really helpful, both for central government departments and local governments. He also flagged that new guidance on how the IG Framework would work in real life, particularly applied to specific vulnerabilities, could be really helpful for other stakeholders to replicate it.
<p>6</p>	<p>Discussion and ask Firoze Salim, CDDO</p>
	<ul style="list-style-type: none"> • Firoze posed a set of questions to the audience, asking working group members to provide answers by writing after the meeting due to time constraints. The questions are: <ul style="list-style-type: none"> ○ Is there anything missing that has not been captured in the product specifications that members feel the group should be addressing? ○ What do members think would be a realistic timescale for the delivery of these products? ○ How can we ensure the group works effectively together? ○ Do members want to lead any of these particular workstreams? ○ Are members happy to publish the meeting notes and to write a blog post to increase transparency and awareness of the work? • With regard to the question of working transparently, a number of members voiced their support for working as openly as possible.
<p>5</p>	<p>Next steps and AOB</p>
	<p>Next Steps</p> <ul style="list-style-type: none"> • CDDO to share the meeting notes with the working group members. • Working group members to provide feedback on the questions asked during the meeting. • Working group members to put forward vulnerability scenarios to be developed under the “Terminology” product specification. • CDDO and SAVVI to publish meeting notes and a blog post <p>Meeting closed</p>

	Next meeting: TBD
--	--------------------------