The Discursive Construction of "Security":

An analysis of the Secure English Language Testing policy in the UK

Johann W. Unger
Luke Harding
Tineke Brunfaut

Context

- **Secure English Language Tests** (SELTs) used for visa and immigration purposes in the UK since 2010

2002: White paper: *Secure borders, safe haven*

2008: Introduction of points-based immigration system

2010: Selection of 12 “Secure English Language Tests” (SELTs)

2010-2011: 1st tender process for SELTs – selection of five SELTs

2013: 2nd tender process initiated

2014: BBC Panorama investigation of cheating / tender process postponed

2015: 2nd tender process finished - selection of two SELTs

The issue

- Traditional meanings of **“test security**” seem to be becoming intertwined with **discourses of border security**

> *We recognise that there is a greater risk of abuse by those seeking to come to the UK to undertake lower level courses of study. Secure English language testing will ensure that we have independent evidence that all education institutions are ensuring their students are capable of following a course delivered in English.*

(UKBA spokesperson, 2010)

- Discursive processes enabling “securitization” (Buzan, Wæver & de Wilde, 1998) of language testing policy in the UK as part of broader **discourse on migration**
- To what extent can language testing research address such phenomena?

Methodological approach

8 steps for discourse-historical analysis:

1. Activation and consultation of preceding **theoretical knowledge** (e.g. about language testing, migration, government policy).
2. Systematic **collection of data and context information** (various texts produced by government, e.g. tender documents, parliamentary debates, media organisations, test providers).
3. **Selection and preparation of data** for specific analyses (careful reading of data and identifying salient sections, e.g. all passages in tender document with instances of "security" and related concepts).
4. Specification of the **research question/s** and formulation of assumptions (on the basis of a literature review and a first skimming of the data).

Based on Reisigl & Wodak, 2015

Methodological approach (cont.)

5. **Qualitative pilot analysis**, including a context analysis, macro-analysis and micro-analysis (allows testing categories and first assumptions, as well as the further specification of assumptions).

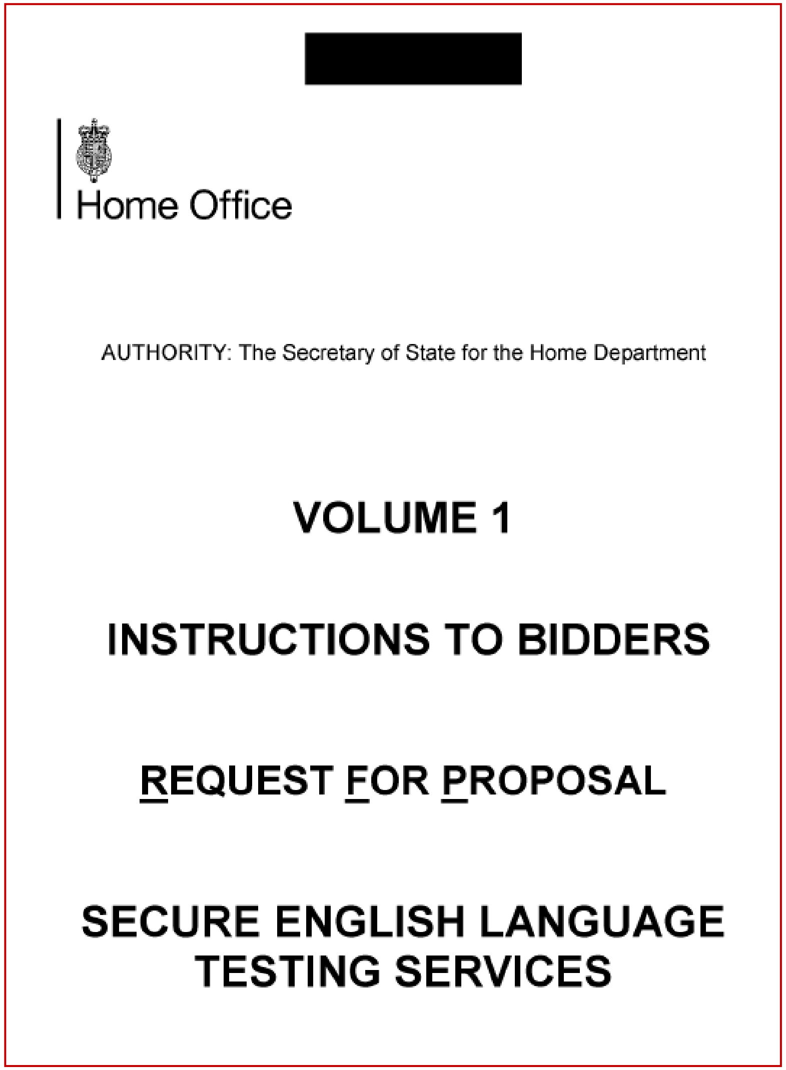
---

6. Detailed **case studies** (of a whole range of data, primarily qualitatively, but in part also quantitatively).
7. Formulation of a **critique** (interpretation and explanation of results, taking into account the relevant context knowledge and referring to the three dimensions of critique).
8. Practical **application** of analytical results (if possible, the results may be applied or proposed for practical application targeting some social impact).

Based on Reisigl & Wodak, 2015

Data

- Set of documents provided in the most recent (2014) **tender** round for selecting Secure English Language Tests, acquired through the *Freedom of Information Act*
- 51 documents
- Partial release of data: some data commercially sensitive, not in public interest (Home Office, personal communication, 2015)



[redacted]

Home Office

AUTHORITY: The Secretary of State for the Home Department

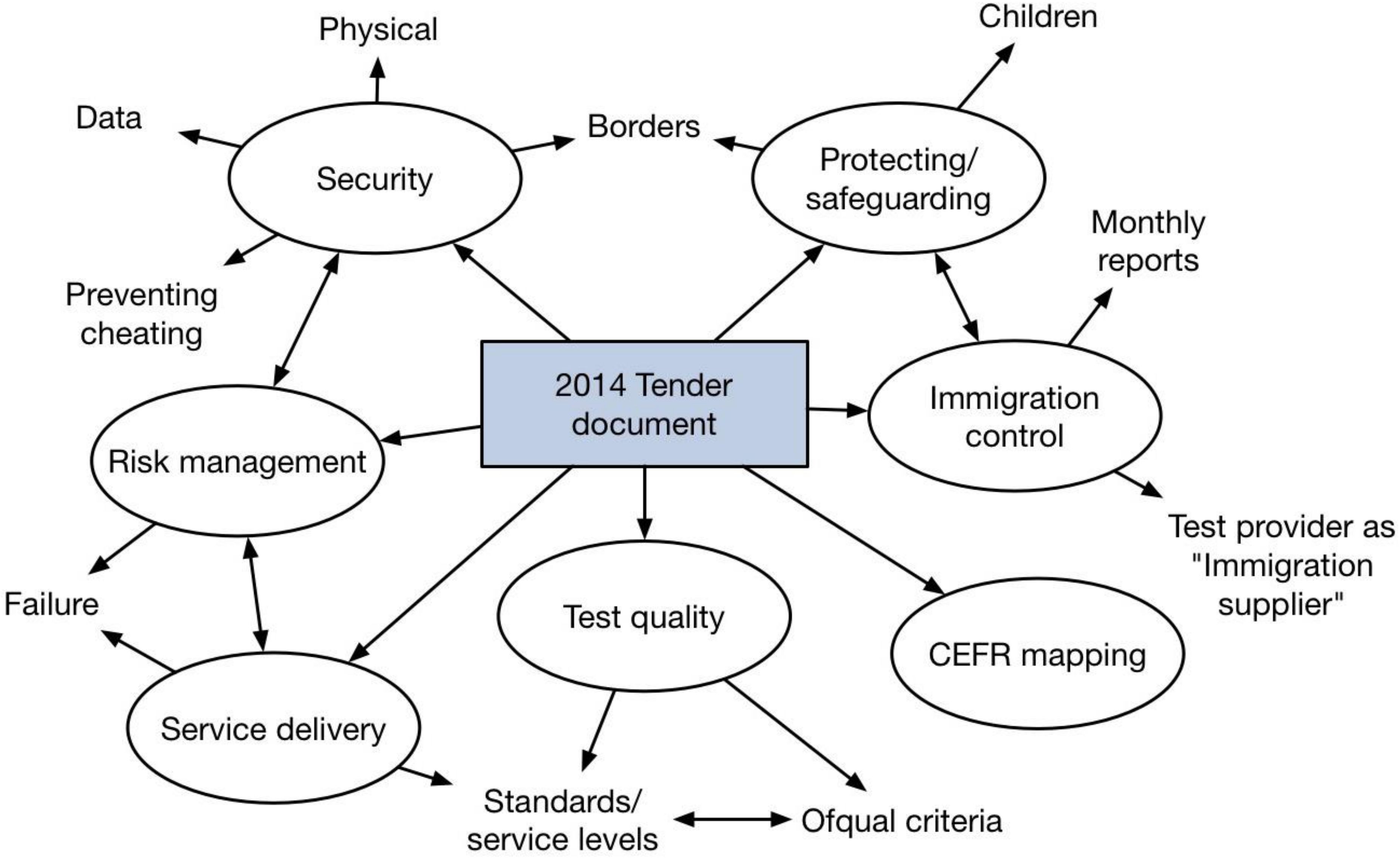
VOLUME 1

INSTRUCTIONS TO BIDDERS

REQUEST FOR PROPOSAL

SECURE ENGLISH LANGUAGE TESTING SERVICES

Topic map



2014 Tender document
Security
Physical
Data
Borders
Preventing cheating
Protecting/ safeguarding
Children
Monthly reports
Immigration control
Test provider as "Immigration supplier"
Risk management
Failure
Service delivery
Test quality
CEFR mapping
Standards/ service levels
Ofqual criteria

Sample analysis:
Security Policy Framework

What is Protective Security?

Protective Security is a risk management process to protect assets and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. The Government processes huge volumes of sensitive information (and personal data to matters of national security) and manages assets and services that are critical to public safety and the UK's way of life. It must guard against a range of threats including negligent behaviours, criminality, terrorism and espionage, as well as natural hazards such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security.

Protective security, particularly with regards to information security, is often expressed in terms of Confidentiality, Integrity and Availability – i.e. that security controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

R-Vol 6-SELT 2.2.3 Understanding Security Policy Framework

Discursive features

- **Generic features of policy texts/legalese**
- Argumentative features including topoi
- Expansion of security beyond testing – semantic fields
- Buzan et al.'s (1998) "securitization"

Sample analysis:
Security Policy Framework

What is Protective Security?

Protective Security is a risk management process to protect assets and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. The Government processes huge volumes of sensitive information (and personal data to matters of national security) and manages assets and services that are critical to public safety and the UK's way of life. It must guard against a range of threats including negligent behaviours, criminality, terrorism and espionage, as well as natural hazards such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security.

Protective security, particularly with regards to information security, is often expressed in terms of **Confidentiality, Integrity and Availability** – i.e. that security controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

R-Vol 6-SELT 2.2.3

Discursive features

- Generic features of policy texts/legalese
- **Argumentative features including topoi**
- Expansion of security beyond testing – semantic fields
- Buzan et al.'s (1998) "securitization"

Sample analysis:
Security Policy Framework

What is Protective Security?

Protective Security is a risk management process to protect assets and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. The Government processes **huge volumes of sensitive information (and personal data** to matters of national security) and manages assets and services that are critical to public safety and the **UK's way of life**. It must **guard against a range of threats** including negligent behaviours, criminality, terrorism and espionage, as well as natural hazards such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security.

Protective security, particularly with regards to information security, is often expressed in terms of Confidentiality, Integrity and Availability – i.e. that security controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

R-Vol 6-SELT 2.2.3

Discursive features

- Generic features of policy texts/legalese
- Argumentative features including topoi
- **Expansion of security beyond testing – semantic fields**
- Buzan et al.'s (1998) "securitization"

Sample analysis:
Security Policy Framework

What is Protective Security?

Protective Security is a risk management process to protect assets and services appropriately, proportionate to threats and in a way that supports (and does not inhibit) business. The Government processes huge volumes of sensitive information (and personal data to matters of national security) and manages assets and services that are critical to public safety and the UK’s way of life. It must guard against a range of threats including negligent behaviours, criminality, **terrorism** and espionage, as well as **natural hazards** such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security.

Protective security, particularly with regards to information security, is often expressed in terms of Confidentiality, Integrity and Availability – i.e. that security controls are effective and that systems and services will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users.

R-Vol 6-SELT 2.2.3

Discursive features

- Generic features of policy texts/legalese
- Argumentative features including topoi
- Expansion of security beyond testing – semantic fields
- **Buzan et al.'s (1998) "securitization"**

Sample analysis:
Security Policy Framework

What is Protective Security?

Protective Security is a risk management process to **protect assets** and services appropriately, **proportionate to threats** and in a way that supports (and does not inhibit) business. The Government processes huge volumes of sensitive information (and personal data to matters of **national security**) and manages assets and services that are critical to public safety and the UK's way of life. It must guard against a range of threats including negligent behaviours, criminality, **terrorism** and espionage, as well as natural hazards such as flooding.

There are three interdependent elements: physical (buildings/estates/property), personnel (including staff) and information (documents/data systems) security.

Protective security, particularly with regards to information security, is often expressed in terms of Confidentiality, Integrity and Availability – i.e. that security controls are effective and that systems and services will protect the information they carry and will **function as they need to, when they need to**, under the control of legitimate users.

R-Vol 6-SELT 2.2.3

Feedback?

http://wp.lancs.ac.uk/ltrg/projects/selt-project/

E-mail	**Twitter**
j.unger@lancaster.ac.uk	@johnnyunger
l.harding@lancaster.ac.uk	@harding_luke
t.brunfaut@lancaster.ac.uk	@TinekeBrunfaut